Administrar un host único de vSphere: VMware Host Client

Actualización 3

Modificado el 29 de julio de 2022

VMware vSphere 7.0

VMware ESXi 7.0

VMware Host Client 1.37.0



Puede encontrar la documentación técnica más actualizada en el sitio web de VMware:

https://docs.vmware.com/es/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Spain, S.L.
Calle Rafael Boti 26
2.ª planta
Madrid 28023
Tel.: +34 914125000
www.vmware.com/es

Contenido

Acerca de la administración de un host único de vSphere: VMware Host Client

Administrar un host único de vSphere: VMware Host Client proporciona información acerca de la administración de hosts individuales con VMware Host Client.

VMware Host Client puede utilizarse para realizar tareas de administración de emergencia cuando vCenter Server no esté disponible. Puede usar VMware Host Client para realizar tareas administrativas, tareas básicas de solución de problemas y tareas administrativas avanzadas.

En VMware, valoramos la inclusión. Para fomentar este principio en nuestros clientes y clientas, partners y comunidad interna, hemos actualizado esta guía para eliminar las instancias de lenguaje no inclusivo.

Audiencia prevista

Esta información está destinada a cualquier usuario que desee utilizar VMware Host Client para administrar hosts ESXi individuales. La información está escrita para administradores del sistema expertos en Windows y Linux que están familiarizados con la tecnología de máquina virtual y las operaciones de centro de datos.

Información actualizada

Esta documentación sobre *Administrar un host único de vSphere: VMware Host Client* se actualiza con cada versión del producto o cuando sea necesario.

En esta tabla se muestra el historial de actualizaciones de *Administrar un host único de vSphere: VMware Host Client*.

Revisión	Descripción
21 de octubre de 2022	Actualizaciones menores en Configurar la puesta a cero de memoria del ámbito del usuario.
19 de octubre de 2022	Actualizaciones menores en Habilite o deshabilite la seguridad basada en la virtualización en una máquina virtual existente en el VMware Host Client.
13 de octubre de 2022	Se eliminaron los espacios en blanco en los fragmentos de código de No se puede establecer la conexión de VMware Host Client a un host ESXi después de actualizar a una versión más reciente de ESXi.
29 de julio de 2022	■ Se actualizaron los requisitos de contraseña de ESXi en Configurar la directiva de bloqueo de cuentas y contraseñas en VMware Host Client. ■ Se actualizó el paso 3 del procedimiento en Configurar el tiempo de espera de la sesión SOAP en VMware Host Client.
26 de mayo de 2022	Información actualizada en Cambiar la configuración de inicio automático en VMware Host Client.
16 de mayo de 2022	Se agregó una captura de pantalla en Generar un paquete de soporte en VMware Host Client.
12 de abril de 2022	Se agregó una captura de pantalla en Usar configuración de columnas de máquinas virtuales en VMware Host Client para mostrar la configuración de columnas.
28 de octubre de 2021	■ Se consolidaron todos los temas que contienen información sobre cómo crear una máquina virtual en Crear una máquina virtual en VMware Host Client. ■ Se consolidaron todos los temas que contienen información sobre cómo implementar una máquina virtual desde un archivo OVF u OVA en Implementar una máquina virtual a partir de un archivo OVF u OVA en VMware Host Client. ■ Se consolidaron todos los temas que contienen información sobre cómo registrar una máquina virtual existente en Registrar una máquina virtual existente en VMware Host Client. ■ Actualización menor a Agregar un usuario de ESXi en VMware Host Client. ■ Actualización menor a Editar la configuración de hora de un host ESXi en VMware Host Client. ■ Se actualizó No se puede establecer la conexión de VMware Host Client a un host ESXi después de actualizar a una versión más reciente de ESXi y se eliminó la información de la versión obsoleta. ■ Se actualizó la tabla Memoria máxima de la máquina virtual en Cambiar la configuración de la memoria. ■ Actualización menor a Cambiar la cantidad de CPU virtuales en VMware Host Client. ■ Se actualizaron los diagramas en Configurar la seguridad de red para iSCSI e iSER y Prácticas recomendadas para configurar redes con iSCSI de software.
05 de octubre de 2021	Versión inicial.

Descripción general de VMware Host Client

1

VMware Host Client es un cliente basado en HTML5 que se usa para conectar y administrar hosts ESXi individuales.

Puede usar VMware Host Client para realizar tareas administrativas y básicas de solución de problemas, además de tareas administrativas avanzadas en el host ESXi de destino. También puede utilizar VMware Host Client para realizar tareas de administración de emergencia cuando vCenter Server no está disponible.

Es importante saber que VMware Host Client es diferente a vSphere Client. vSphere Client se usa para conectarse a vCenter Server y administrar varios hosts ESXi, mientras que VMware Host Client se usa para administrar un solo host ESXi.

Las funciones de VMware Host Client incluyen, entre otras, las siguientes operaciones:

- Operaciones básicas de virtualización, como implementación y configuración de máquinas virtuales de variada complejidad
- Crear y administrar redes y almacenes de datos
- Ajuste avanzado de las opciones de niveles de host para mejorar el rendimiento

Este capítulo incluye los siguientes temas:

Requisitos del sistema de VMware Host Client

Asegúrese de que su explorador sea compatible con VMware Host Client.

Los siguientes sistemas operativos invitados y las siguientes versiones de exploradores web son compatibles con VMware Host Client.

Exploradores compatibles	Mac OS	Windows de 32 bits y 64 bits	Linux
Google Chrome	89+	89+	75+
Mozilla Firefox	80+	80+	60+

Exploradores compatibles	Mac OS	Windows de 32 bits y 64 bits	Linux
Microsoft Edge	90+	90+	N/C
Safari	9.0+	N/C	N/C

Usar VMware Host Client

La instancia integrada de VMware Host Client es un cliente basado en HTML5 que solo se usa para administrar hosts ESXi únicos. Puede utilizar VMware Host Client para realizar tareas de administración de emergencia cuando vCenter Server no está disponible temporalmente.

Inicie VMware Host Client e inicie sesión.

Puede usar VMware Host Client para administrar hosts ESXi individuales y realizar varias tareas administrativas y de solución de problemas en sus máquinas virtuales.

Nota VMware Host Client solamente funciona para los usuarios con privilegios administrativos.

Procedimiento

1 En un explorador web, introduzca el nombre o la dirección IP del host de destino con el formato **`http://`*`nombre-de-host`*`/ui`** o **`http://`*`dirección-IP-de-host`*`/ui`**.

   Aparecerá un registro en la pantalla.

2 Escriba su nombre de usuario y su contraseña.

3 Haga clic en **Iniciar sesión** para continuar.

4 Revise la página del Programa para la mejora de la experiencia del cliente (CEIP) de VMware y elija si desea unirse al programa.

   Para obtener más información sobre el programa y cómo configurarlo en cualquier momento, consulte Configurar el Programa de mejora de la experiencia del cliente.

5 Haga clic en **Aceptar**.

Resultados

Ha iniciado sesión en el host ESXi de destino.

Cerrar sesión en VMware Host Client

Cuando ya no necesite ver ni administrar el host ESXi de destino, cierre la sesión de VMware Host Client.

Nota El cierre de la sesión de VMware Host Client no detiene el host.

Procedimiento

- Para cerrar sesión en el host ESXi, haga clic en el nombre de usuario desde la parte superior de la ventana de VMware Host Client y seleccione **Cerrar sesión** en el menú desplegable.

  Ha cerrado la sesión en VMware Host Client. El host ESXi de destino continúa ejecutando todas sus actividades normales.

Configurar el Programa de mejora de la experiencia del cliente

Puede participar en el Programa de mejora de la experiencia de cliente (CEIP) para proporcionar comentarios o información anónimos a VMware para mejorar la calidad, la fiabilidad y la funcionalidad de los productos y servicios de VMware.

Programa de mejora de la experiencia de cliente de VMware

VMware Tools participa en el Programa de mejora de la experiencia de cliente de (CEIP) de VMware.

Los detalles relacionados con los datos recopilados mediante el CEIP, así como los fines para los que VMware los utiliza, se pueden encontrar en el Centro de seguridad y confianza en http://www.vmware.com/trustvmware/ceip.html.

Abandonar el Programa de mejora de la experiencia del cliente o volver a unirse a él en VMware Host Client

Puede abandonar el Programa de mejora de la experiencia del cliente (CEIP) o volver a unirse a él en cualquier momento.

Procedimiento

1 Para abandonar el CEIP y volver a unirse a él, haga clic en el nombre de usuario en la parte superior de la página de VMware Host Client.

2 Apunte a **Configuración del cliente**> **Enviar estadísticas de uso** para abandonar el CEIP o volver a unirse a él.

Administrar hosts con VMware Host Client

2

Con VMware Host Client, puede administrar hosts ESXi individuales durante las actualizaciones de vCenter Server o cuando vCenter Server deja de responder o no está disponible.

VMware Host Client cuenta con un conjunto esencial de funciones de solución de problemas que le permiten realizar tareas en el host ESXi en el que ha iniciado sesión si vCenter Server está disponible. Estas funciones incluyen la configuración de opciones avanzadas de host, la asignación de licencias, la administración de certificados, el uso de ESXi Shell, la habilitación del modo de bloqueo, etc.

Este capítulo incluye los siguientes temas:

Administrar la configuración del sistema en VMware Host Client

Con VMware Host Client, puede administrar la configuración avanzada del host, asignar licencias al host o quitárselas, configurar directivas de inicio y detención para servicios de host, y administrar la configuración de fecha y hora del host.

Administrar opciones de configuración avanzadas en VMware Host Client

Puede cambiar la configuración de un host mediante VMware Host Client.

Precaución No se admite la modificación de opciones avanzadas a menos que el soporte técnico de VMware o un artículo de la base de conocimientos le otorgue instrucciones para hacerlo. En todos los otros casos, no se admite el cambio de estas opciones. En la mayoría de los casos, la configuración predeterminada proporciona resultados óptimos.

Procedimiento

1. Haga clic en **Administrar** desde el inventario de VMware Host Client y, a continuación, haga clic en **Sistema**.
2. Haga clic en **Configuración avanzada**.
3. Haga clic con el botón derecho en el elemento correspondiente de la lista y seleccione **Editar opción** en el menú desplegable.

   Aparece el cuadro de dialogo de **Editar opción**.
4. Edite los valores y haga clic en **Guardar** para aplicar los cambios.
5. (opcional) Haga clic con el botón derecho en el elemento adecuado en la lista y seleccione **Restablecer valores predeterminados** para restituir la configuración original del elemento.

Crear un mensaje de bienvenida inicial para la interfaz de usuario de la consola directa y VMware Host Client

Al utilizar VMware Host Client, puede crear un mensaje de bienvenida que aparezca en la pantalla inicial de la interfaz de usuario de la consola directa (DCUI) y en la ventana de inicio de sesión de VMware Host Client. También puede crear un mensaje de bienvenida que aparezca después de que un usuario inicie sesión en VMware Host Client y decida si desea mostrar el mensaje de bienvenida.

Procedimiento

1 Haga clic en **Administrar** desde el inventario de VMware Host Client y, a continuación, haga clic en **Configuración avanzada**.

Opción	Acción
Cree un mensaje de bienvenida que aparezca antes de iniciar sesión en DCUI y VMware Host Client	a Introduzca **`Annotations.WelcomeMessage`** en el cuadro de texto **Buscar** y haga clic en el icono **Buscar**. b Haga clic con el botón secundario en `Annotations.WelcomeMessage` y seleccione **Editar opción** en el menú desplegable. Se abrirá entonces el cuadro de diálogo **Editar opción**. c En el cuadro de texto **Nuevo valor**, introduzca el mensaje de bienvenida. Para establecer el mensaje predeterminado, deje en blanco el cuadro de texto **Nuevo valor**.
Cree un mensaje de bienvenida que aparezca después de iniciar sesión en VMware Host Client	a Introduzca **`UserVars.HostClientWelcomeMessage`** en el cuadro de texto **Buscar** y haga clic en el icono **Buscar**. b Haga clic con el botón secundario en `UserVars.HostClientWelcomeMessage` y seleccione **Editar opción** en el menú desplegable. Se abrirá entonces el cuadro de diálogo **Editar opción**. c En el cuadro de texto **Nuevo valor**, introduzca el mensaje de bienvenida. Para establecer el mensaje predeterminado, deje en blanco el cuadro de texto **Nuevo valor**.
Habilite o deshabilite la visualización del mensaje de bienvenida después de iniciar sesión en VMware Host Client	a Introduzca **`UserVars.HostClientEnableMOTDNotification`** en el cuadro de texto **Buscar** y haga clic en el icono **Buscar**. b Haga clic con el botón secundario en `UserVars.HostClientEnableMOTDNotification` y seleccione **Editar opción** en el menú desplegable. Se abrirá entonces el cuadro de diálogo **Editar opción**. c En el cuadro de texto **Nuevo valor**, introduzca el nuevo valor. Un valor de cero (0) deshabilita la visualización del mensaje de bienvenida. Un valor de uno (1) habilita la visualización del mensaje de bienvenida.

2 Haga clic en **Guardar**.

3 (opcional) Para restablecer la configuración de clave predeterminada, haga clic con el botón derecho en la clave adecuada de la lista y seleccione **Restablecer al valor predeterminado**.

Configurar el tiempo de espera de la sesión de la interfaz de usuario de VMware Host Client

En VMware Host Client, el tiempo de espera de la sesión de la interfaz de usuario se agota automáticamente cada 15 minutos y, a continuación, debe volver a iniciar sesión en VMware Host Client.

Puede aumentar el tiempo de espera de inactividad predeterminado cambiando un parámetro de configuración avanzada. El valor predeterminado es 900 segundos.

Procedimiento

- Configure el tiempo de espera de la sesión de la interfaz de usuario.

Opción	Acción
En la configuración avanzada de VMware Host Client	a Haga clic en **Administrar** desde el inventario de VMware Host Client y, a continuación, haga clic en **Configuración avanzada** b Introduzca **`UserVars.HostClientSessionTimeout`** en el cuadro de texto **Buscar** y haga clic en el icono **Buscar**. c Haga clic con el botón secundario en `UserVars.HostClientSessionTimeout` y seleccione **Editar opción** en el menú desplegable. Se abrirá entonces el cuadro de diálogo **Editar opción**. d En el cuadro de texto **Nuevo valor**, introduzca la configuración de tiempo de espera en segundos. **Nota** Un valor de cero (0) deshabilita el tiempo de inactividad. e Haga clic en **Guardar**. f (opcional) Para restablecer la configuración de clave predeterminada, haga clic con el botón derecho en la clave adecuada de la lista y seleccione **Restablecer al valor predeterminado**.
En el menú desplegable Configuración de usuario	a Haga clic en el nombre de usuario en la parte superior de la ventana de VMware Host Client y seleccione **Configuración > Tiempo de espera de aplicación > .** b Para especificar el tiempo de espera de inactividad, seleccione la hora. c Para deshabilitar el tiempo de espera de inactividad, seleccione `Off`.

Configurar el tiempo de espera de la sesión SOAP en VMware Host Client

En VMware Host Client, puede configurar el tiempo de espera de la sesión SOAP.

Procedimiento

1 Haga clic en **Administrar** desde el inventario de VMware Host Client y, a continuación, haga clic en **Configuración avanzada**.

2 Introduzca **`Config.HostAgent.vmacore.soap.sessionTimeout`** en el cuadro de texto **Buscar** y haga clic en el icono **Buscar**.

3 Haga clic con el botón secundario en `Config.HostAgent.vmacore.soap.sessionTimeout` y seleccione **Editar opción** en el menú desplegable.

   Se abrirá entonces el cuadro de diálogo **Editar opción**.

4 En el cuadro de texto **Nuevo valor**, introduzca la configuración de tiempo de espera en segundos.

   Un valor de cero (0) desactiva el tiempo de espera.

5 Haga clic en **Guardar**.

6 (opcional) Para restablecer la configuración de clave predeterminada, haga clic con el botón secundario en la clave adecuada de la lista y seleccione **Restablecer al valor predeterminado**.

Configurar la directiva de bloqueo de cuentas y contraseñas en VMware Host Client

Para los hosts ESXi, debe utilizar una contraseña con requisitos predefinidos. Puede cambiar la longitud de contraseña requerida y los requisitos de clases de caracteres, o permitir frases de contraseña utilizando la opción avanzada `Security.PasswordQualityControl`. También puede establecer el número de contraseñas para recordar para cada usuario mediante la opción avanzada `Security.PasswordHistory`. La opción avanzada `Security.PasswordMaxDays` permite configurar el número máximo de días entre cambios de contraseña.

Nota Después de cambiar la configuración de contraseña predeterminada, siempre realice una prueba adicional.

Si intenta iniciar sesión con credenciales incorrectas, la política de bloqueo de cuentas especifica cuándo y durante cuánto tiempo el sistema bloquea su cuenta.

Contraseñas de ESXi

ESXi aplica los requisitos de contraseña para el acceso.

- De forma predeterminada, al crear una contraseña, se debe incluir una combinación de tres de cualquiera de las cuatro siguientes clases de caracteres: letras minúsculas, letras mayúsculas, números y caracteres especiales, como guion bajo o raya.
- De forma predeterminada, la contraseña debe tener una longitud de al menos 7 caracteres y un máximo de 40 caracteres.
- Las contraseñas no deben contener una palabra de diccionario ni parte de una palabra de diccionario.
- Las contraseñas no deben contener el nombre de usuario ni partes del mismo.

Nota Un carácter en mayúscula al inicio de una contraseña no se tiene en cuenta en la cantidad de clases de caracteres que se utilizan. Un número al final de una contraseña no se tiene en cuenta en la cantidad de clases de caracteres que se utilizan.

Ejemplo de contraseñas de ESXi

Las siguientes contraseñas ilustran posibles contraseñas si la opción está configurada de la siguiente manera:

```
retry=3 min=disabled,disabled,disabled,7,7
```

Con esta opción, se solicita al usuario hasta tres veces (retry=3) una contraseña nueva si no es lo suficientemente segura o si la contraseña no se introdujo correctamente dos veces. No se permiten las contraseñas que tienen una o dos clases de caracteres ni las frases de contraseña, ya que los primeros tres elementos están desactivados. Las contraseñas de tres y cuatro clases requieren 7 caracteres.

Las siguientes contraseñas posibles cumplen con los requisitos de contraseña:

- xQaTEhb!: contiene ocho caracteres de tres clases.
- xQaT3#A: contiene siete caracteres de cuatro clases.

Las siguientes contraseñas posibles no cumplen con los requisitos de contraseña:

- Xqat3hi: comienza con un carácter en mayúscula, lo que reduce la cantidad efectiva de clases de caracteres a dos. La cantidad mínima de clases de caracteres requerida es tres.
- xQaTEh2: termina con un número, lo que reduce la cantidad efectiva de clases de caracteres a dos. La cantidad mínima de clases de caracteres requerida es tres.

Control de calidad de contraseña

Puede controlar la calidad de las contraseñas mediante la opción avanzada `Security.PasswordQualityControl`.

`Security.PasswordQualityControl` consta de varias opciones que siguen el patrón:

```
retry=N min=N0,N1,N2,N3,N4 max=N passphrase=N similar=permit|deny
```

Ajustes de control de calidad de contraseña	Descripción	Predeterminado
retry=N	El número de veces que el usuario debe proporcionar una nueva contraseña si la contraseña es incorrecta o no es lo suficientemente segura.	retry=3
min=N0,N1,N2,N3,N4	Requisito de longitud mínima de frase de contraseña y clase de caracteres. ■ N0 es la longitud mínima de contraseñas de una sola clase de carácter. ■ N1 es la longitud mínima de contraseñas de dos clases de caracteres. ■ N2 es la longitud mínima de una frase de contraseña. ■ N3 es la longitud mínima de tres clases. ■ N4 es la longitud mínima de cuatro clases. Puede utilizar disabled para deshabilitar una contraseña con el número especificado de clases de caracteres.	min=disabled,disabled,disabled,7,7
max=N	La longitud máxima de contraseña permitida.	max=40
passphrase=N	El número de palabras requeridas para una frase de contraseña. Para asegurarse de que se reconozca la passphrase, no establezca N2 de la opción min en disabled.	passphrase=3
similar=permit|deny	Indica si una contraseña puede ser similar a la contraseña anterior. Para usar esta opción, asegúrese de establecer la opción Security.PasswordHistory en un valor distinto de cero.	similar=deny

Frase de contraseña de ESXi

En lugar de una contraseña, puede usar una frase de contraseña. Las frases de contraseña están desactivadas de forma predeterminada. Puede cambiar el valor predeterminado usando la opción avanzada Security.PasswordQualityControl.

Por ejemplo, puede cambiar la opción por la siguiente.

```
retry=3 min=disabled,disabled,16,7,7
```

Este ejemplo permite frases de contraseña de al menos 16 caracteres. La frase de contraseña debe constar de al menos 3 palabras, separadas por espacios.

Ejemplo de historial de contraseñas y directiva de rotación

Para recordar un historial de 5 contraseñas, establezca la opción `Security.PasswordHistory` en 5.

Para aplicar una directiva de rotación de contraseñas de 90 días, establezca la opción de `Security.PasswordMaxDays` en 90.

Activar directiva de bloqueo de cuentas ESXi

Los usuarios quedan bloqueados después de una cantidad preestablecida de intentos consecutivos con errores. De manera predeterminada, los usuarios quedan bloqueados después de 5 intentos consecutivos fallidos en 3 minutos, y una cuenta bloqueada se desbloquea automáticamente transcurridos 15 minutos de forma predeterminada. Puede cambiar el número máximo de intentos fallidos permitidos y el período de tiempo en el que la cuenta de usuario está bloqueada mediante las opciones avanzadas `Security.AccountLockFailures` y `Security.AccountUnlockTime`.

Para configurar las contraseñas de administrador y el comportamiento de bloqueo de cuentas, lleve a cabo los siguientes pasos.

Procedimiento

1 Haga clic en **Administrar** desde el inventario de VMware Host Client y, a continuación, haga clic en **Configuración avanzada**.

Opción	Acción
Configure la longitud de contraseña requerida, el requisito de clase de caracteres o permita frases de contraseña	a Introduzca **`Security.PasswordQualityControl`** en el cuadro de texto **Buscar** y haga clic en el icono **Buscar**. b Haga clic con el botón secundario en `Security.PasswordQualityControl` y seleccione **Editar opción** en el menú desplegable.
Configurar el número de contraseñas que se recordarán para cada usuario	a Introduzca **`Security.PasswordHistory`** en el cuadro de texto **Buscar** y haga clic en el icono **Buscar**. b Haga clic con el botón secundario en `Security.PasswordHistory` y seleccione **Editar opción** en el menú desplegable. **Nota** Cero desactiva el historial de contraseñas.
Configurar el número máximo de días entre cambios de contraseña	a Introduzca **`Security.PasswordMaxDays`** en el cuadro de texto **Buscar** y haga clic en el icono **Buscar**. b Haga clic con el botón secundario en `Security.PasswordMaxDays` y seleccione **Editar opción** en el menú desplegable.

Opción	Acción
Configurar el número de intentos de inicio de sesión fallidos permitidos antes del bloqueo	a Introduzca **`Security.AccountLockFailures`** en el cuadro de texto **Buscar** y haga clic en el icono **Buscar**. b Haga clic con el botón secundario en `Security.AccountLockFailures` y seleccione **Editar opción** en el menú desplegable. **Nota** Cero (0) desactiva el bloqueo de cuentas.
Configurar el período de tiempo durante el cual se bloquea la cuenta del usuario	a Introduzca **`Security.AccountUnlockTime`** en el cuadro de texto **Buscar** y haga clic en el icono **Buscar**. b Haga clic con el botón secundario en `Security.AccountUnlockTime` y seleccione **Editar opción** en el menú desplegable.

Se abrirá entonces el cuadro de diálogo **Editar opción**.

2 En el cuadro de texto **Nuevo valor**, introduzca la nueva opción.

3 Haga clic en **Guardar**.

4 (opcional) Para restablecer la configuración de clave predeterminada, haga clic con el botón secundario en la clave adecuada de la lista y seleccione **Restablecer al valor predeterminado**.

Configurar syslog en VMware Host Client

Para configurar el servicio syslog, puede utilizar VMware Host Client.

Procedimiento

1 Haga clic en **Administrar** desde el inventario de VMware Host Client y, a continuación, haga clic en **Configuración avanzada**.

2 En el cuadro de texto **Buscar**, introduzca el nombre de la opción que desea cambiar y haga clic en el icono **Buscar**.

Opción	Descripción
Syslog.global.LogHost	El host remoto al que se reenvían los mensajes de syslog y el puerto en el que el host remoto recibe mensajes de syslog. Puede incluir el protocolo y el puerto, por ejemplo, `protocol://hostName1:port` donde `protocol` puede ser udp, tcp o ssl. Solo puede utilizar el puerto 514 para UDP. El protocolo SSL utiliza TLS 1.2. Por ejemplo: `ssl://hostName1:1514`. El valor de `port` puede ser cualquier número decimal entre 1 y 65535. Si bien no existe un límite estricto para la cantidad de hosts remotos que recibirán mensajes de Syslog, se recomienda mantener el número de hosts remotos en cinco o menos.
Syslog.global.logCheckSSLCerts	Fuerce la comprobación de certificados SSL al iniciar sesión en un host remoto.
Syslog.global.defaultRotate	Cantidad máxima de archivos que desea guardar. Puede configurar este número en forma global y para subregistradores individuales.
Syslog.global.defaultSize	Tamaño predeterminado del registro, en KB, antes de que el sistema rote los registros. Puede configurar este número en forma global y para subregistradores individuales.

Opción	Descripción
Syslog.global.LogDir	El directorio en el que se almacenan los registros. El directorio puede encontrarse en volúmenes NFS o VMFS montados. Solo el directorio `/scratch` del sistema de archivos local se mantiene en todos los reinicios. Especifique el directorio como [*nombrealmacéndatos*] *ruta_a_archivo*, donde la ruta de acceso es relativa a la raíz del volumen que respalda el almacén de datos. Por ejemplo, la ruta de acceso `[storage1] /systemlogs` se asigna a la ruta de acceso `/vmfs/volumes/storage1/systemlogs`.
Syslog.global.logDirUnique	Al seleccionar esta opción, se crea un subdirectorio con el nombre del host ESXi del directorio especificado por **Syslog.global.LogDir**. Un directorio único es útil si varios hosts ESXi utilizan el mismo directorio NFS.

3 Haga clic con el botón secundario en el nombre de la opción y seleccione **Editar opción** en el menú desplegable.

   Se abrirá entonces el cuadro de diálogo **Editar opción**.

4 Para realizar la comprobación de certificados SSL al iniciar sesión en un host remoto, haga clic en **True** en el **nuevo valor**.

5 Haga clic en **Guardar**.

6 (opcional) Para restablecer la configuración de clave predeterminada, haga clic con el botón derecho en la clave adecuada de la lista y seleccione **Restablecer al valor predeterminado**.

Configurar opciones avanzadas de clave TLS/SSL

Puede configurar los protocolos de seguridad y los algoritmos criptográficos que se utilizan para cifrar las comunicaciones con el host ESXi.

La clave de seguridad de la capa de transporte (TLS) protege la comunicación con el host mediante el protocolo TLS. Tras el primer arranque, el host ESXi genera la clave TLS como una clave RSA de 2048 bits. Actualmente, ESXi no implementa la generación automática de claves ECDSA para TLS. La clave privada de TLS no está pensada para que el administrador la procese.

La clave SSH protege la comunicación con el host ESXi mediante el protocolo SSH. Tras el primer arranque, el sistema genera la clave SSH como una clave RSA de 2048 bits. El servidor SSH está desactivado de forma predeterminada. El acceso SSH está destinado principalmente a fines de solución de problemas. La clave SSH no está pensada para que el administrador la procese. El inicio de sesión a través de SSH requiere privilegios administrativos equivalentes al control total del host. Para habilitar el acceso SSH, consulte Habilitar Secure Shell (SSH) en VMware Host Client.

Puede establecer los siguientes parámetros de clave de seguridad del host ESXi.

Clave	Predeterminado	Descripción
UserVars.ESXiVPsAllowedCiphers	! aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES	La cadena de control de cifrado predeterminada.
UserVars.ESXiVPsDisabledProtocols	sslv3,tlsv1,tlsv1.1	De forma predeterminada, habilita los protocolos TLS v1.0, v1.1 y v1.2. SSL v3.0 está deshabilitado. Si no especifica un protocolo, se habilitan todos.
Config.HostAgent.ssl.keyStore.allowAny	False	Puede agregar cualquier certificado al almacén de confianza de la entidad de certificación de ESXi.
Config.HostAgent.ssl.keyStore.allowSelfSigned	False	Puede agregar certificados autofirmados que no sean de entidad de certificación al almacén de confianza de entidades de certificación de ESXi, es decir, a los certificados que no tienen el bit de entidad de certificación establecido.
Config.HostAgent.ssl.keyStore.discardLeaf	True	Descarta los certificados de hoja agregados al almacén de confianza de entidades de certificación de ESXi.

Para establecer los ajustes de clave de seguridad de ESXi:

Procedimiento

1 Haga clic en **Administrar** desde el inventario de VMware Host Client y, a continuación, haga clic en **Configuración avanzada**.

2 Introduzca la clave de seguridad en el cuadro de texto **Buscar** y haga clic en el icono **Buscar**.

3 Haga clic con el botón secundario en la clave de seguridad y seleccione **Editar opción** en el menú desplegable.

   Se abrirá entonces el cuadro de diálogo **Editar opción**.

4 En el campo **Nuevo valor** entre el nuevo valor y haga clic en **Guardar**.

5 (opcional) Para restablecer la configuración de clave predeterminada, haga clic con el botón derecho en la clave adecuada de la lista y seleccione **Restablecer al valor predeterminado**.

Configurar la puesta a cero de memoria del ámbito del usuario

Con VMware Host Client, puede utilizar la opción avanzada `Mem.MemEagerZero` para determinar cómo se ponen a cero las páginas de las máquinas virtuales y aplicaciones de espacio de usuario.

Para poner a cero todas las páginas cuando se asignan a máquinas virtuales y aplicaciones de espacio de usuario, establezca `Mem.MemEagerZero` en cero (1). Si no se reutiliza la memoria, esta configuración impide que se exponga la información de una máquina virtual o aplicaciones de espacio de usuario a otros clientes mientras se conserva el contenido anterior en la memoria.

Cuando se establece `Mem.MemEagerZero` en 1, las páginas se ponen a cero cuando se cierra una aplicación de espacio de usuario. Para las máquinas virtuales, estas páginas se ponen a cero en las siguientes circunstancias:

- La máquina virtual está apagada.
- Se migran las páginas de la máquina virtual.
- El host ESXi recupera la memoria de las máquinas virtuales.

Nota Para las máquinas virtuales, puede obtener este comportamiento estableciendo la opción avanzada `sched.mem.eagerZero` en **`TRUE`**.

Para obtener información sobre la configuración de las opciones avanzadas de la máquina virtual, consulte la documentación *Administrar recursos de vSphere*.

Para configurar la puesta a cero de memoria del ámbito del usuario, realice los siguientes pasos.

Procedimiento

1. Haga clic en **Administrar** desde el inventario de VMware Host Client y, a continuación, haga clic en **Configuración avanzada**.
2. Introduzca **`Mem.MemEagerZero`** en el cuadro de texto **Buscar** y haga clic en el icono **Buscar**.
3. Haga clic con el botón secundario en `Mem.MemEagerZero` y seleccione **Editar opción** en el menú desplegable.

   Se abrirá entonces el cuadro de diálogo **Editar opción**.
4. En el cuadro de texto **Nuevo valor**, introduzca el nuevo valor.

   El valor predeterminado es cero (0).
5. Haga clic en **Guardar**.
6. (opcional) Para restablecer la configuración de clave predeterminada, haga clic con el botón secundario en la clave adecuada de la lista y seleccione **Restablecer al valor predeterminado**.

Cambiar la configuración de inicio automático en VMware Host Client

Configure las opciones de inicio automático para que el host ESXi se instale cuando se inicie o detenga el host.

Procedimiento

1. Haga clic en **Administrar** desde el inventario de VMware Host Client y, a continuación, haga clic en **Sistema**.

2 Haga clic en **Inicio automático**.

3 Haga clic en **Editar configuración**.

4 Seleccione **Sí** para habilitar el cambio de configuración de inicio automático.

Opción	Descripción
Retraso al iniciar	Después de iniciar el host ESXi, este enciende las máquinas virtuales que están configuradas con el inicio automático. Después de que el host ESXi enciende la primera máquina virtual, espera el tiempo de demora especificado y, a continuación, enciende la siguiente máquina virtual.
Retraso al detener	El retraso al detener es el período máximo durante el cual el host ESXi espera a que se complete un comando de apagado. El orden en el que se apagan las máquinas virtuales es el contrario al orden de inicio. Una vez que el host ESXi apaga la primera máquina virtual dentro del período especificado, el host apaga la siguiente máquina virtual. Si una máquina virtual no se apaga dentro del período de demora especificado, el host ejecuta un comando de apagado y, a continuación, comienza a apagar la siguiente máquina virtual. El host ESXi se apaga solo después de que se hayan apagado todas las máquinas virtuales.
Detener acción	Seleccione una acción de apagado que se aplique a las máquinas virtuales del host cuando este último se apague. ■ **Valor predeterminado del sistema** ■ **Apagar** ■ **Suspender** ■ **Apagar**
Esperar latido	Seleccione **Sí** para habilitar la opción **Esperar latido**. Puede usar esta opción si el sistema operativo invitado de la máquina virtual tiene VMware Tools instalado. Después de que el host ESXi enciende la primera máquina virtual, el host enciende inmediatamente la siguiente máquina virtual. El orden de inicio en el que se encienden las máquinas virtuales continúa después de que la máquina virtual reciba el primer latido.

Si establece una opción de retraso en `-1`, el sistema utiliza la opción predeterminada.

5 Haga clic en **Guardar**.

Editar la configuración de hora de un host ESXi en VMware Host Client

Mediante el uso de VMware Host Client, puede configurar manualmente la configuración de hora de un host o puede sincronizar la hora y la fecha del host con un servidor NTP o PTP. NTP proporciona una precisión de sincronización de milisegundos y PTP mantiene la precisión de sincronización de microsegundos.

El servicio NTP en el host toma periódicamente la fecha y la hora del servidor NTP. Puede utilizar los botones **Iniciar**, **Detener** o **Reiniciar** para cambiar el estado del servicio NTP en el host en cualquier momento, independientemente de la directiva de inicio seleccionada para el servicio NTP.

PTP proporciona una sincronización horaria precisa a las máquinas virtuales dentro de una red. Para cambiar el servicio PTP en el host en cualquier momento, puede utilizar los botones **Iniciar**, **Detener** o **Reiniciar**. Al iniciar o detener el servicio PTP, se habilita o deshabilita PTP automáticamente. Para aplicar el cambio cuando habilite o deshabilite PTP manualmente, inicie o detenga el servicio PTP.

Para obtener más información sobre los servicios, consulte Administrar servicios en VMware Host Client.

Nota Los servicios NTP y PTP no se pueden ejecutar al mismo tiempo.

Procedimiento

1 Haga clic en **Administrar** en el inventario de VMware Host Client.

2 En la pestaña **Sistema**, haga clic en **Hora y fecha**.

3 Configure la fecha y la hora del host.

Opción	Acción
Configurar manualmente la fecha y hora en este host	a Haga clic en **Editar configuración de NTP**. Se mostrará el cuadro de diálogo **Editar configuración de NTP**. b Configurar manualmente la fecha y hora del host. c Haga clic en **Guardar**.
Usar protocolo de hora de red (Habilitar el cliente NTP)	a Haga clic en **Editar configuración de NTP**. Se mostrará el cuadro de diálogo **Editar configuración de NTP**. b Seleccione el botón de opción **Usar protocolo de hora de red**. c En el cuadro de texto **Servidores NTP**, escriba las direcciones IP o los nombres de host de los servidores NTP que desea usar. d En el menú desplegable **Directiva de inicio del servicio NTP**, seleccione una opción para iniciar y detener el servicio NTP en el host. ■ **Iniciar y detener con uso del puerto**: inicia o detiene el servicio NTP cuando el puerto del cliente NTP se habilita o deshabilita para el acceso en el perfil de seguridad del host. ■ **Iniciar y detener con el host**: inicia o detiene el servicio NTP cuando se enciende y apaga el host. ■ **Iniciar y detener manualmente**. Habilita el inicio y la detención manual del servicio NTP. Si selecciona la directiva **Iniciar y detener manualmente**, el estado del servicio NTP solamente cambiará al usar los controles de la interfaz de usuario. e Haga clic en **Guardar**.
Usar protocolo de hora de precisión (Habilitar el cliente PTP)	a Haga clic en **Editar configuración de PTP**. b Active la casilla **Habilitar**. c En el menú desplegable **Interfaz de red**, seleccione una interfaz de red. Aparecen IPv4 y máscara de subred. d Haga clic en **Guardar**.

Administrar hardware para un host ESXi mediante VMware Host Client

Al iniciar sesión en un host ESXi mediante VMware Host Client, puede administrar dispositivos PCI y configurar las opciones de administración de energía.

Directivas de administración de energía del host

Puede aplicar diversas características de administración de energía en ESXi que el hardware de host proporciona para ajustar el equilibrio entre rendimiento y energía. Para controlar de qué forma ESXi utiliza estas características, seleccione una directiva de administración de energía.

Al seleccionar una directiva de alto rendimiento, se proporciona más rendimiento absoluto, pero menos eficiencia (rendimiento por vatio). Las directivas de energía reducida proporcionan menos rendimiento absoluto, pero más eficiencia.

Puede seleccionar una directiva para el host que administra mediante VMware Host Client. Si no selecciona ninguna directiva, ESXi utiliza la directiva Equilibrado de forma predeterminada.

Tabla 2-1. Directivas de administración de energía de la CPU

Directiva de administración de energía	Descripción
Alto rendimiento	No utiliza ninguna característica de administración de energía.
Equilibrado (valor predeterminado)	Reduce el consumo de energía con mínimo perjuicio del rendimiento
Poca energía	Reduce el consumo de energía con riesgo de rendimiento bajo
Personalizado	Directiva de administración de energía definida por el usuario. Están disponibles las opciones de configuración avanzada.

Cuando una CPU se ejecuta en una frecuencia más baja, también puede ejecutarse con un voltaje más bajo, lo cual ahorra energía. Este tipo de administración de energía suele denominarse ajuste dinámico de voltaje y frecuencia (DVFS). ESXi intenta ajustar las frecuencias de CPU de modo que el rendimiento de la máquina virtual no se vea afectado.

Cuando una CPU está inactiva, ESXi puede aplicar estados de interrupción profunda, también conocidos como estados C. Cuanto más profundo es el estado C, menos energía utiliza la CPU, pero, a la vez, más tarda en reanudar su ejecución. Cuando una CPU se vuelve inactiva, ESXi aplica un algoritmo para predecir la dirección del estado inactivo y elige un estado C adecuado en el cual entrar. En las directivas de administración de energía que no utilizan estados C profundos, ESXi solamente utiliza el estado de interrupción menos profundo en las CPU inactivas (C1).

Cambiar las directivas de administración de energía en VMware Host Client

Cambie las directivas de administración de energía del host que está administrando para controlar el consumo de energía del host.

Procedimiento

1. Haga clic en **Administrar** desde el inventario de VMware Host Client y, a continuación, haga clic en **Hardware**.
2. Haga clic en **Administración de energía** y, a continuación, en **Cambiar directiva**.

   Se muestran las directivas de administración de energía disponibles.
3. Seleccione el botón de opción que aparece junto a la directiva que desea aplicar.
4. Haga clic en **Aceptar**.

Cambiar la etiqueta de hardware en VMware Host Client

En VMware Host Client, puede cambiar la etiqueta de hardware de todos los dispositivos de acceso directo PCI disponibles en una máquina virtual. Las etiquetas de hardware se utilizan para restringir la colocación de la máquina virtual en instancias de hardware específicas. Puede agregar todos los dispositivos disponibles con la misma etiqueta de hardware o con una etiqueta de hardware en blanco a una máquina virtual.

Procedimiento

1. Haga clic en **Administrar** en el inventario de VMware Host Client.
2. En la pestaña **Hardware**, haga clic en **Dispositivos PCI**.
3. Seleccione un dispositivo disponible de la lista y haga clic en **Etiqueta de hardware**.

   El acceso directo debe estar habilitado para el dispositivo seleccionado.

   Se mostrará el cuadro de diálogo **Editar etiqueta de hardware**.
4. Edite la etiqueta de hardware y haga clic en **Guardar** para aplicar los cambios.

Resultados

La nueva etiqueta de hardware aparece en la columna de etiqueta de hardware.

Licencias para hosts ESXi

Los hosts ESXi tienen licencias de vSphere. Cada licencia de vSphere tiene una cierta capacidad que usted puede usar para concederles licencias a varias CPU físicas en hosts ESXi.

A partir de vSphere 7.0, una licencia de CPU abarca una CPU con hasta 32 núcleos. Si una CPU tiene más de 32 núcleos, necesitará licencias de CPU adicionales.

Cantidad de CPU	Núcleos por CPU	Número de licencias de CPU
1	1-32	1
2	1-32	2
1	33-64	2
2	33-64	4

Cuando se asigna una licencia de vSphere a un host, la cantidad de capacidad consumida se determina en función del número de CPU físicas en el host y la cantidad de núcleos en cada CPU física. La instancia de vSphere Desktop que está destinada a entornos de VDI se otorga con licencia por cada máquina virtual individual.

Para conceder una licencia a un host ESXi, debe asignarle una licencia de vSphere que cumpla los siguientes requisitos previos:

- La licencia debe tener capacidad suficiente para conceder licencias a todas las CPU físicas del host.
- La licencia debe admitir todas las características que utiliza el host. Por ejemplo, si el host está asociado con vSphere Distributed Switch, la licencia que le asigne debe admitir la característica vSphere Distributed Switch.

Si intenta asignarle una licencia con capacidad insuficiente o que no admite las características que usa el host, se producirá un error en la asignación de la licencia.

Si utiliza el modelo de concesión de licencias con hasta 32 núcleos, puede asignar una licencia de vSphere para 10 CPU de 32 núcleos a cualquiera de las siguientes combinaciones de hosts:

- Cinco hosts con 2 CPU y 32 núcleos por CPU
- Cinco hosts con 1 CPU y 64 núcleos por CPU
- Dos hosts con 2 CPU y 48 núcleos por CPU y dos hosts con 1 CPU y 20 núcleos por CPU

Las CPU de doble núcleo o cuatro núcleos, como las CPU Intel que combinan dos o cuatro CPU independientes en un único chip, cuentan como una sola CPU.

Modo de evaluación

Después de instalar ESXi, funciona en modo de evaluación durante un máximo de 60 días consecutivos. Una licencia de modo de evaluación proporciona todas las características de la edición del producto vSphere de gama más alta.

Después de asignar una licencia a un host ESXi, en cualquier momento antes de que caduque el período de evaluación, puede volver a establecer el host en el modo de evaluación para explorar todo el conjunto de características disponibles durante el período de evaluación restante.

Por ejemplo, si usa un host ESXi en modo de evaluación durante 20 días, luego asigna una licencia de vSphere Standard al host y 5 días después vuelve a configurar el host en el modo de evaluación, puede explorar todo el conjunto de características que están disponibles para el host durante el período de evaluación restante de 35 días.

Caducidad del período de evaluación y licencia

Cuando expira el período de evaluación o la licencia de los hosts ESXi, estos se desconectan de vCenter Server. Todas las máquinas virtuales que estén encendidas continúan funcionando, pero no puede encender las máquinas virtuales una vez que se apagan. No puede cambiar la configuración actual de las características que están en uso. No se pueden utilizar las características que permanecieron sin usar antes de la caducidad de la licencia.

Nota Cuando haya licencias a punto de caducar, aparecerá una notificación 90 días antes de que la licencia caduque.

Licencias para hosts ESXi tras la actualización

Si actualiza un host ESXi a una versión que comienza con el mismo número, no es necesario que reemplace la licencia existente por una nueva. Por ejemplo, si actualiza un host desde ESXi 5.1 a 5.5, puede utilizar la misma licencia para el host.

Si actualiza un host ESXi a una versión superior que comienza con un número distinto, se reinicia el período de evaluación y se debe asignar una licencia nueva. Por ejemplo, si actualiza un host ESXi de 5.x a 6.x, el host debe incluir una licencia de vSphere 6.

vSphere Desktop

vSphere Desktop está pensado para entornos de VDI, como Horizon View. El uso de licencias para vSphere Desktop es igual al número de máquinas virtuales de escritorio encendidas que se ejecutan en los hosts a los que se les asigna una licencia de vSphere Desktop.

Ver información de licencias sobre el entorno de VMware Host Client

Puede ver las licencias disponibles en VMware Host Client, junto con sus fechas de caducidad, su clave de licencia y varias características más. También puede ver los productos y los activos disponibles.

Procedimiento

- Haga clic en **Administrar** desde el inventario de VMware Host Client y, a continuación, haga clic en **Conceder licencias**.

  Puede ver la clave de licencia, la fecha de caducidad, y todas las funciones y los activos disponibles.

Asignar una clave de licencia a un host ESXi en VMware Host Client

Mediante VMware Host Client, se puede asignar una clave de licencia nueva o existente a un host ESXi.

Requisitos previos

Compruebe que posee el privilegio **Global.Licencias**.

Nota Si utiliza vCenter Server para administrar el host ESXi, solo podrá cambiar las licencias desde vSphere Client.

Procedimiento

1 Haga clic en **Administrar** desde el inventario de VMware Host Client y, a continuación, haga clic en **Conceder licencias**.

2 Haga clic en **Asignar licencia**, introduzca una clave de licencia con el formato ***XXXXX-XXXXX-XXXXX-XXXXX-XXXXX*** y, a continuación, haga clic en **Comprobar licencia**.

3 Haga clic en **Asignar licencia** para guardar los cambios.

Quitar una licencia de un host ESXi en VMware Host Client

Para seguir cumpliendo con los modelos de licencia de los productos que usa con vSphere, debe quitar del inventario todas las licencias no asignadas. Si dividió, combinó o actualizó licencias en Customer Connect, deberá quitar las licencias anteriores.

Por ejemplo, supongamos que actualizó una licencia de vSphere de 6.5 a 6.7 en Customer Connect. Asigna una licencia de vSphere a hosts ESXi 6.7. Después de asignar las nuevas licencias de vSphere 6.7, deberá quitar del inventario la licencia anterior de vSphere 6.5.

Procedimiento

1 Haga clic en **Administrar** desde el inventario de VMware Host Client y, a continuación, haga clic en **Conceder licencias**.

2 Haga clic en **Quitar licencia** y, a continuación, haga clic en **Aceptar**.

Administrar servicios en VMware Host Client

En VMware Host Client, puede iniciar, detener y reiniciar los servicios que se ejecutan en el host en el que ha iniciado sesión, y puede configurar directivas de servicio de host. Puede reiniciar servicios al cambiar una configuración o en caso de sospecha de problemas funcionales o de rendimiento.

Procedimiento

1 Haga clic en **Administrar** desde el inventario de VMware Host Client y, a continuación, haga clic en **Servicios**.

2 En la lista **Servicios**, seleccione un servicio.

3 En el menú desplegable **Acciones**, seleccione una operación.

   - **Reiniciar**
   - **Iniciar**

- **Detener**

4 (opcional) En el menú desplegable **Acciones**, seleccione **Directiva** y, a continuación, seleccione una opción de servicio en el menú.

   - **Iniciar y detener con puertos de firewall**
   - **Iniciar y detener con el host**
   - **Iniciar y detener manualmente**

Administrar seguridad y usuarios para un host ESXi mediante VMware Host Client

La arquitectura del hipervisor de ESXi cuenta con varias características integradas que se pueden configurar para mejorar la seguridad. Mediante VMware Host Client, puede configurar características como Active Directory y, además, administrar certificados.

Administrar la autenticación de host mediante VMware Host Client

Al iniciar sesión en un host ESXi mediante VMware Host Client, puede comprobar si están habilitadas la autenticación de Active Directory y la autenticación de tarjeta inteligente, además de unir el host a un dominio de servicio de directorio.

Unir un host ESXi a un dominio de servicio de directorio mediante VMware Host Client

Si desea utilizar un servicio de directorio para su host, se debe unir el host al dominio del servicio de directorio.

Es posible introducir el nombre de dominio con uno de los dos métodos siguientes:

- **`name.tld`** (por ejemplo, **`domain.com`**): la cuenta se crea en el contenedor predeterminado.
- **`name.tld/container/path`** (por ejemplo, **`domain.com/OU1/OU2)`**: la cuenta se crea en una unidad organizativa (OU) en particular.

Para utilizar el servicio vSphere Authentication Proxy, consulte *Seguridad de vSphere*.

Procedimiento

1 Haga clic en **Administrar** desde el inventario de VMware Host Client y, a continuación, haga clic en **Seguridad y usuarios**.

2 Haga clic en **Autenticación** y, a continuación, en **Unirse al dominio**.

3 Introduzca un nombre de dominio.

   Utilice el formulario **`name.tld`** o **`name.tld/container/path`**.

4 Introduzca el nombre de usuario y la contraseña de la cuenta de usuario de servicio de directorio que tenga permisos para unir el host al dominio y, a continuación, haga clic en **Unirse al dominio**.

5 (opcional) Si desea utilizar un proxy de autenticación, introduzca la dirección IP del servidor proxy y haga clic en **Unirse al dominio**.

Usar Active Directory para administrar usuarios de ESXi

Se puede configurar ESXi para utilizar un servicio de directorio como Active Directory con el fin de administrar usuarios.

La creación de cuentas de usuarios locales en cada host presenta desafíos para la sincronización de los nombres y las contraseñas de las cuentas en varios hosts. Conecte los hosts ESXi a un dominio de Active Directory para que no sea necesario crear y mantener cuentas de usuarios locales. La utilización de Active Directory para autenticar usuarios simplifica la configuración del host ESXi y reduce el riesgo de que ocurran problemas de configuración que podrían permitir un acceso no autorizado.

Al utilizar Active Directory, los usuarios suministran sus credenciales de Active Directory y el nombre de dominio del servidor de Active Directory cuando se agrega un host a un dominio.

Usar vSphere Authentication Proxy

Se pueden agregar hosts ESXi a un dominio de Active Directory mediante vSphere Authentication Proxy en lugar de agregarlos explícitamente al dominio de Active Directory.

Solo tiene que configurar el host de manera que conozca el nombre de dominio del servidor de Active Directory y la dirección IP de vSphere Authentication Proxy. Cuando vSphere Authentication Proxy está habilitado, automáticamente agrega hosts que se aprovisionan con Auto Deploy al dominio de Active Directory. También puede usar vSphere Authentication Proxy con hosts que no se aprovisionan mediante Auto Deploy.

Consulte la documentación de *Seguridad de vSphere* para obtener información sobre cómo habilitar vSphere Authentication Proxy y qué puertos de vCenter Server requiere vSphere Authentication Proxy.

Auto Deploy

Si aprovisiona hosts con Auto Deploy, puede configurar un host de referencia que apunte a Authentication Proxy. A continuación, debe configurar una regla que aplique el perfil del host de referencia a cualquier host ESXi que esté aprovisionado con Auto Deploy. vSphere Authentication Proxy almacena las direcciones IP de todos los hosts que Auto Deploy aprovisiona mediante PXE en la lista de control de acceso. Cuando el host arranca, se pone en contacto con vSphere Authentication Proxy, el cual une esos hosts, que ya están en la lista de control de acceso, al dominio de Active Directory.

Incluso si usa vSphere Authentication Proxy en un entorno que utiliza certificados aprovisionados por VMCA o certificados de terceros, el proceso funciona sin problemas si sigue las instrucciones para usar certificados personalizados con Auto Deploy.

Otros hosts ESXi

Se pueden configurar otros hosts para que usen vSphere Authentication Proxy si desea permitir que el host se una al dominio sin usar credenciales de Active Directory. Es decir, no

necesita transmitir credenciales de Active Directory al host ni guardar credenciales de Active Directory en el perfil de host.

En ese caso, debe agregar la dirección IP del host a la lista de control de acceso de vSphere Authentication Proxy para que este autorice el host según su dirección IP predeterminada. Puede habilitar la autenticación del cliente para que vSphere Authentication Proxy realice la verificación del certificado del host.

Nota No se puede utilizar vSphere Authentication Proxy en un entorno compatible solo con IPv6.

Administrar certificados de host mediante VMware Host Client

Al iniciar sesión en host ESXi mediante VMware Host Client, puede ver los detalles de certificación de su host, como el emisor y el período de validez, y también importar certificados.

Ver detalles de certificados para un host ESXi en VMware Host Client

Puede utilizar la información del certificado para la depuración.

Procedimiento

1 Haga clic en **Administrar** desde el inventario de VMware Host Client y, a continuación, haga clic en **Seguridad y usuarios**.

2 Haga clic en **Certificados**.

Puede ver los siguientes detalles de certificados.

Campo	Descripción
Emisor	El emisor del certificado.
No válido después de	La fecha en la que caduca el certificado.
No válido antes de	La fecha en la que se generó el certificado.
Asunto	El asunto usado durante la generación del certificado.

Importar un certificado nuevo para un host ESXi en VMware Host Client

Puede importar un certificado de una entidad de certificación de confianza al iniciar sesión en un host ESXi con VMware Host Client.

Procedimiento

1 Haga clic en **Administrar** desde el inventario de VMware Host Client y, a continuación, haga clic en **Seguridad y usuarios**.

2 Haga clic en **Certificados** y, a continuación, haga clic en **Importar nuevo certificado**.

3 Genere una solicitud de firma del certificado:

Opción	Descripción
Generar solicitud de firma de FQDN	■ Haga clic en **Generar solicitud de firma de FQDN**, haga clic en el botón **Copiar en el portapapeles** y, a continuación, haga clic en **Cerrar**. ■ Para generar el certificado firmado, pase la solicitud de firma del certificado a la entidad de certificación (CA). ■ En el cuadro de texto **Certificado**, pegue el certificado firmado generado en formato PEM y haga clic en **Importar**.
Generar solicitud de firma de IP	■ Haga clic en **Generar solicitud de firma de IP**, haga clic en el botón **Copiar en el portapapeles** y, a continuación, haga clic en **Cerrar**. ■ Para generar el certificado firmado, pase la solicitud de firma del certificado a la CA. ■ En el cuadro de texto **Certificado**, pegue el certificado firmado generado en formato PEM y haga clic en **Importar**.

No tiene que importar el certificado inmediatamente. Para asegurarse de que puede utilizar el certificado firmado, no reinicie el host entre generar la solicitud de firma del certificado e importar el certificado.

La solicitud de firma de certificado luego se envía a una entidad de certificación para generar el certificado oficial.

Una solicitud de FQDN tiene el nombre de host completo del host en el campo de nombre común resultante del certificado. La solicitud de firma de IP tiene la dirección actual del host en el campo de nombre común.

Administrar usuarios con VMware Host Client

Administre los usuarios para controlar quién está autorizado a iniciar sesión en ESXi.

Los usuarios y las funciones controlan quién tiene acceso a los componentes del host ESXi y qué acciones puede realizar cada usuario.

En vSphere 5.1 y posterior, la administración de usuarios de ESXi presenta las siguientes advertencias.

- Los usuarios que se crean cuando se establece una conexión directa con un host ESXi no son los mismos que los usuarios de vCenter Server. Cuando vCenter Server administra el host, vCenter Server omite los usuarios creados directamente en el host.
- No es posible crear usuarios de ESXi con vSphere Client. Debe iniciar sesión directamente en el host con VMware Host Client para crear usuarios de ESXi.
- ESXi 5.1 y posterior no son compatibles con los grupos locales. No obstante, sí son compatibles con los grupos de Active Directory.

Para evitar que un usuario anónimo, como root, acceda al host con la interfaz de usuario de la consola directa (DCUI) o con ESXi Shell, elimine los privilegios de administrador del usuario en la carpeta raíz del host. Esto es válido tanto para los usuarios locales como para los usuarios y grupos de Active Directory.

Agregar un usuario de ESXi en VMware Host Client

Al agregar un usuario a la tabla de usuarios se actualiza la lista interna de usuarios que mantiene el host.

Requisitos previos

Para obtener más información sobre los requisitos de contraseña, consulte la documentación de Configurar la directiva de bloqueo de cuentas y contraseñas en VMware Host Client o *Seguridad de vSphere*

Procedimiento

1 Inicie sesión en ESXi con VMware Host Client.

No es posible crear usuarios de ESXi con vSphere Client. Para crear usuarios de ESXi, debe iniciar sesión directamente en el host con VMware Host Client.

2 Haga clic en **Administrar** desde el inventario de VMware Host Client y, a continuación, haga clic en **Seguridad y usuarios**.

3 Haga clic en **Usuarios**.

4 Haga clic en **Agregar usuario**.

5 Escriba un nombre de usuario y una contraseña.

Nota No cree un usuario con nombre **ALL**. Es posible que los privilegios asociados con el nombre **ALL** no estén disponibles para todos los usuarios en algunos casos. Por ejemplo, si un usuario con nombre **TODOS** tiene privilegios de administrador, es posible que un usuario con privilegios **Solo lectura** pueda iniciar sesión en el host de forma remota. Este no es el comportamiento previsto.

- No incluya espacios en el nombre de usuario.
- No incluya en el nombre de usuario caracteres que no sean ASCII.
- Cree una contraseña que cumpla con los requisitos de longitud y complejidad. El host comprueba el cumplimiento de la contraseña mediante el complemento de autenticación predeterminado, `pam_passwdqc.so`. Si la contraseña no cumple con los requisitos, aparece un mensaje de error.

6 Haga clic en **Agregar**.

Actualizar un usuario de ESXi en VMware Host Client

Puede cambiar la descripción y la contraseña de un usuario de ESXi en VMware Host Client.

Procedimiento

1 Haga clic en **Administrar** desde el inventario de VMware Host Client y, a continuación, haga clic en **Seguridad y usuarios**.

2 Haga clic en **Usuarios**.

3 Seleccione un usuario de la lista y haga clic en **Editar usuario**.

4 Actualice los detalles del usuario y haga clic en **Guardar**.

Quitar un usuario local de ESXi de un host de VMware Host Client

Se puede quitar un usuario local de ESXi del host.

Precaución No quite al usuario raíz.

Si quita un usuario del host, este pierde los permisos para todos los objetos del host y no puede volver a iniciar sesión.

Nota Los usuarios que están conectados y se eliminan del dominio conservan los permisos del host hasta que el host se reinicie.

Procedimiento

1 Haga clic en **Administrar** desde el inventario de VMware Host Client y, a continuación, haga clic en **Seguridad y usuarios**.

2 Haga clic en **Usuarios**.

3 Seleccione el usuario que desea quitar de la lista, haga clic en **Quitar usuario** y, por último, en **Sí**.

   No quite al usuario raíz por ningún motivo.

Administrar funciones de ESXi en VMware Host Client

ESXi otorga acceso a los objetos únicamente a los usuarios que tienen asignados permisos para el objeto en cuestión. Para asignar a un usuario un permiso para el objeto, debe emparejar un usuario con una función. Una función es un conjunto predefinido de privilegios. Para obtener más información sobre los privilegios, consulte la documentación *Seguridad de vSphere*.

Los hosts ESXi proporcionan tres roles predeterminados, cuyos privilegios asociados no pueden cambiarse. Cada rol predeterminado posterior incluye los privilegios del rol anterior. Por ejemplo, la función de administrador hereda los privilegios de la función de solo lectura. Las funciones que se crean no heredan los privilegios de otras funciones predeterminadas.

Si desea crear funciones personalizadas, puede utilizar las opciones de edición de funciones de VMware Host Client para crear conjuntos de privilegios que coincidan con las necesidades del usuario. Asimismo, las funciones que se crean directamente en un host no son accesibles en vCenter Server. Para poder trabajar con estas funciones, se debe iniciar sesión en el host directamente desde VMware Host Client.

Nota Cuando se agrega una función personalizada y no se le asignan privilegios, la función creada es de solo lectura con los privilegios **Anónimo.Sistema**, **Ver.Sistema** y **Leer.Sistema** definidos por el sistema.

Si administra un host ESXi a través de vCenter Server, el mantenimiento de funciones personalizadas tanto en el host como en vCenter Server puede provocar confusión y una utilización incorrecta. En este tipo de configuración, mantenga los roles personalizados únicamente en vCenter Server.

Se pueden crear funciones para el host y establecer permisos a través de una conexión directa con el host ESXi mediante VMware Host Client.

Agregar una función en VMware Host Client

Puede crear funciones que se adapten a las necesidades de control de acceso del entorno.

Requisitos previos

Asegúrese de haber iniciado sesión como usuario con privilegios de administrador, como raíz o vpxuser.

Procedimiento

1 Haga clic en **Administrar** desde el inventario de VMware Host Client y, a continuación, haga clic en **Seguridad y usuarios**.
2 Haga clic en **Funciones**.
3 Haga clic en **Agregar función**.
4 Escriba un nombre para la nueva función.
5 Seleccione de la lista los privilegios que desee asociar con la nueva función y haga clic en **Agregar**.

Actualizar una función en VMware Host Client

Cuando se edita una función, se pueden cambiar los privilegios seleccionados para esa función. Una vez completado este paso, los privilegios se aplican a todos los usuarios o grupos a los que se haya asignado la función editada.

Requisitos previos

Asegúrese de haber iniciado sesión como usuario con privilegios de administrador, como raíz o vpxuser.

Procedimiento

1 Haga clic en **Administrar** desde el inventario de VMware Host Client y, a continuación, haga clic en **Seguridad y usuarios**.
2 Haga clic en **Funciones**.
3 Seleccione una función de la lista y haga clic en **Editar función**.
4 Actualice los detalles de la función y haga clic en **Guardar**.

Quitar una función en VMware Host Client

Cuando quita un rol que no está asignado a ningún usuario ni grupo, la definición se elimina de la lista de roles. Cuando quita un rol que está asignado a un usuario o un grupo, puede quitar asignaciones o reemplazarlas con una asignación a otro rol.

Precaución Debe comprender de qué forma se verán afectados los usuarios antes de eliminar todas las asignaciones o reemplazarlas. Los usuarios a quienes no se han otorgado permisos no pueden iniciar sesión.

Requisitos previos

Asegúrese de haber iniciado sesión como usuario con privilegios de administrador, como raíz o vpxuser.

Procedimiento

1. Haga clic en **Administrar** desde el inventario de VMware Host Client y, a continuación, haga clic en **Seguridad y usuarios**.
2. Haga clic en **Funciones**.
3. Seleccione el nombre de la función que desea quitar de la lista.
4. Haga clic en **Quitar función**, seleccione **Eliminar solo si no está en uso** y haga clic en **Sí**.

Administrar hosts en vCenter Server

Para supervisar todos los hosts del entorno virtual desde un solo lugar y para simplificar la configuración del host, conecte los hosts a un sistema vCenter Server.

Para obtener información sobre cómo administrar la configuración de hosts ESXi, consulte la documentación de *Redes de vSphere*, de *Almacenamiento de vSphere* y de *Seguridad de vSphere*.

Actualizar entorno de VMware Host Client a la versión más reciente

Para determinar si está utilizando la versión más reciente de VMware Host Client, compruebe qué VIB están instalados en su entorno y examine la información de las versiones de los VIB. Puede actualizar el entorno de VMware Host Client introduciendo una URL o una ruta de almacén de datos a un VIB o al archivo `metadata.zip` en un paquete ESXi sin conexión.

Si proporciona un archivo VIB, el VIB existente que está instalado en el entorno de VMware Host Client se actualiza al VIB nuevo.

Si proporciona un paquete sin conexión, actualiza todo el host ESXi a la versión descrita por el archivo `metadata.zip` en el paquete. Asegúrese de que todo el paquete sin conexión esté disponible a través de la URL o esté cargado en el almacén de datos.

Procedimiento

- Para actualizar el entorno a la versión más reciente, realice las siguientes tareas:

Tarea	Pasos
Cargar un VIB en un almacén de datos	a Haga clic en **Almacenamiento** en el entorno de VMware Host Client. b Seleccione un almacén de datos en la lista y haga clic en **Explorador de almacenes de datos**. c Para almacenar el VIB, seleccione un directorio y haga clic en **Cargar**. d Busque y haga doble clic en el archivo.
Cargar un paquete sin conexión a un almacén de datos	a Descargue el paquete ESXi sin conexión. b Cargue el paquete de ESXi sin conexión en el host ESXi. Puede cargar el paquete de paquetes sin conexión mediante el **Explorador de almacenes de datos** o mediante SCP o WinSCP. c Extraiga el contenido del paquete sin conexión en el host ESXi. Por ejemplo, inicie sesión en el host mediante SSH. d Desplácese hasta el directorio donde cargó el paquete sin conexión. e Extraiga el contenido mediante el `unzip` comando.
Actualizar el entorno	a Haga clic en **Administrar** en VMware Host Client y en **Paquetes**. b Haga clic en **Instalar actualización** e introduzca la URL o la ruta del almacén de datos a un VIB o a un archivo `metadata.zip` en un paquete sin conexión. c Haga clic en **Actualizar**. **Precaución** Si actualiza un host ESXi administrado por vSphere Lifecycle Manager, es posible que el host deje de cumplir los requisitos. d Haga clic en **Actualizar** para asegurarse de que la actualización se haya ejecutado correctamente.

No se puede establecer la conexión de VMware Host Client a un host ESXi después de actualizar a una versión más reciente de ESXi

Después de actualizar el host de ESXi a una versión más reciente, la consola del explorador puede mostrar un mensaje de error al intentar acceder al host de ESXi mediante VMware Host Client, y la conexión puede presentar errores.

Problema

Después de actualizar el host ESXi a una versión más reciente, al intentar desplazarse a **`https://host-fqdn/ui`** o **`https://1.2.3.4/ui`** puede producir el siguiente error:

```
503 Servicio no disponible (no se pudo establecer la conexión con el endpoint:
[N7Vmacore4Http16LocalServiceSpecE:0xffa014e8] _serverNamespace = /ui _isRedirect = false
_port = 8308)
```

Causa

Cualquier cambio en `/etc/vmware/rhttpproxy/endpoints.conf` se conserva después de una actualización y provoca que el endpoint `/ui` anule la instancia de VMware Host Client.

Cuando falta la porción `/ticket` en el archivo `endpoint.conf` del host ESXi 6.0 o posterior, la consola de la máquina virtual en el explorador muestra el mensaje de error `No se pudo establecer la conexión`, pero VMware Remote Console sigue funcionando.

Solución

1 Inicie sesión en el host ESXi por medio de SSH o de ESXi Shell.

   Si utiliza SSH, es posible que primero deba habilitarlo. Puede hacerlo mediante DCUI.

2 Realice una copia de seguridad del archivo `endpoints.conf`.

```
cp /etc/vmware/rhttpproxy/endpoints.conf /tmp
```

3 Abra el archivo `/etc/vmware/rhttpproxy/endpoints.conf` en un editor y elimine la siguiente línea.

```
/ui local 8308 redirect  allow
```

4 Reinicie el servidor de administración de configuración **rhttpproxy**.

```
/etc/init.d/rhttpproxy restart
```

5 Acceda al VMware Host Client mediante el nombre completo especificado del host en la URL segura con **`https://host-fqdn/ui`** o una dirección IP numérica válida **`https://1.2.3.4/ui`**.

Cambiar al vSphere Client

Para acceder al conjunto completo de funcionalidades, funciones administrativas avanzadas y funciones de solución de problemas del host ESXi, conecte el host ESXi a vCenter Server.

Procedimiento

1 Haga clic con el botón derecho en **Host** desde el inventario de VMware Host Client y seleccione **Administrar con vCenter Server** en el menú desplegable.

   La página de inicio de sesión de vCenter Server se abre en una nueva ventana.

2 Introduzca las credenciales y haga clic en **Iniciar sesión**.

Desconectar un host ESXi de vCenter Server mediante VMware Host Client

Si ya no desea usar más el conjunto avanzado de funcionalidades que están disponibles mediante vCenter Server para administración de hosts, o si ha ocurrido un error con vCenter Server y

debe realizar operaciones de emergencia en el host, puede desconectar su host ESXi de vCenter Server.

Desconectar un host ESXi puede tardar varios minutos.

Procedimiento

1 Haga clic con el botón derecho en **Host** desde el inventario de VMware Host Client y seleccione **Desconectar de vCenter Server** en el menú emergente.

   Nota La desconexión de un host le indica a vCenter Server que el host no responde.

2 Haga clic en **Desconectar de vCenter Server**.

Reiniciar o apagar un host ESXi en VMware Host Client

Puede apagar o reiniciar cualquier host ESXi mediante VMware Host Client. Al apagar un host administrado, este se desconecta de vCenter Server, pero no se quita del inventario.

Requisitos previos

Para poder reiniciar o apagar un host, necesitará estos privilegios.

- **Host.Configuración.Mantenimiento**
- **Global.Registrar evento**

Realice siempre las siguientes tareas antes de reiniciar o apagar un host:

- Apague todas las máquinas virtuales en el host.
- Coloque el host en modo de mantenimiento.

Procedimiento

1 Haga clic con el botón derecho en el host y seleccione **Apagar host** o **Reiniciar host**.

   Nota Si el host no está en modo de mantenimiento, apagarlo o reiniciarlo no detiene de manera segura las máquinas virtuales que están en ejecución en ese host y pueden perderse los datos no guardados. Si el host es parte de en un clúster de vSAN, es posible que pierda el acceso a los datos de vSAN en el host.

2 Haga clic en **Apagar** o en **Reiniciar**.

Usar ESXi Shell

ESXi Shell está deshabilitado de manera predeterminada en los hosts ESXi. Es posible habilitar el acceso local y remoto al shell, si es necesario.

Para reducir el riesgo de accesos no autorizados, habilite ESXi Shell solo para solucionar problemas.

ESXi Shell es independiente del modo de bloqueo. Incluso si el host se ejecuta en modo de bloqueo, todavía puede iniciar sesión en ESXi Shell si está habilitado.

Consulte *Seguridad de vSphere*.

ESXi Shell

Habilite este servicio para acceder a ESXi Shell de forma local.

SSH

Habilite este servicio para acceder a ESXi Shell de forma remota mediante SSH.

El usuario raíz y los usuarios con la función de administrador pueden acceder a ESXi Shell. Los usuarios que se encuentran en el grupo de Administradores de ESX reciben automáticamente la función de administrador. De forma predeterminada, solamente el usuario raíz puede ejecutar comandos del sistema (como `vmware -v`) mediante ESXi Shell.

Nota No habilite ESXi Shell a menos que necesite el acceso.

Habilitar Secure Shell (SSH) en VMware Host Client

Habilite Secure Shell (SSH) para acceder a ESXi Shell de manera remota mediante SSH.

Procedimiento

1 Para habilitar o deshabilitar Secure Shell (SSH), haga clic con el botón derecho en **Host** desde el inventario de VMware Host Client.

2 Seleccione **Servicios** en el menú desplegable y, a continuación, **Secure Shell (SSH)**.

3 Seleccione una tarea para realizar.

- Si SSH está habilitado, haga clic en **Deshabilitar** para deshabilitarlo.
- Si SSH está deshabilitado, haga clic en **Habilitar** para habilitarlo.

Habilitar el shell de consola de ESXi en VMware Host Client

Cuando este servicio se habilita mientras se está ejecutando en modo de bloqueo, se puede iniciar sesión de forma local en la interfaz de usuario de consola directa como usuario raíz y deshabilitar el modo de bloqueo. Posteriormente, se puede acceder al host con una conexión directa a VMware Host Client o habilitando ESXi Shell.

Procedimiento

1 Para habilitar o deshabilitar el shell de consola, haga clic con el botón derecho en **Host** desde el inventario de VMware Host Client.

2 Seleccione **Servicios** en el menú desplegable y, a continuación, **Shell de consola**.

3 Seleccione una tarea para realizar.

- Si el shell de consola está habilitado, haga clic en **Deshabilitar** para deshabilitarlo.

- Si el shell de consola está deshabilitado, haga clic en **Habilitar** para habilitarlo.

Crear un tiempo de espera de disponibilidad de ESXi Shell en VMware Host Client

El shell ESXi está deshabilitado de forma predeterminada. Para aumentar la seguridad cuando se habilita el shell, puede establecer un tiempo de espera de disponibilidad para el shell ESXi.

El tiempo de espera de disponibilidad define cuánto tiempo se permiten los inicios de sesión locales y remotos del shell antes de que se deshabilite la capacidad para iniciar sesión a través del shell. Cuando caduca el tiempo de espera de disponibilidad, se mantienen las sesiones del shell existentes, pero no se permiten nuevas.

Procedimiento

1. Haga clic en **Administrar** desde el inventario de VMware Host Client y, a continuación, haga clic en **Configuración avanzada**.
2. Introduzca **`UserVars.ESXiShellTimeOut`** en el cuadro de texto **Buscar** y haga clic en el icono **Buscar**.
3. Haga clic con el botón secundario en `UserVars.ESXiShellTimeOut` y seleccione **Editar opción** en el menú desplegable.

   Se abrirá entonces el cuadro de diálogo **Editar opción**.
4. En el cuadro de texto **Nuevo valor**, introduzca la configuración de tiempo de espera.

   Un valor de cero (0) deshabilita el tiempo de inactividad.
5. Haga clic en **Guardar**.

   Debe reiniciar el servicio SSH y el servicio del shell ESXi para que se aplique el tiempo de espera.
6. (opcional) Para restablecer la configuración de clave predeterminada, haga clic con el botón derecho en la clave adecuada de la lista y seleccione **Restablecer al valor predeterminado**.

Crear un tiempo de espera para sesiones de ESXi Shell inactivas en VMware Host Client

Si habilita ESXi Shell en un host, pero olvida cerrar la sesión, la sesión inactiva permanece conectada de forma indefinida. La conexión abierta aumenta las posibilidades de que alguien obtenga acceso privilegiado al host ESXi. Para impedir esta situación, configure un tiempo de espera para las sesiones inactivas.

El tiempo de espera de inactividad corresponde a la cantidad de tiempo que puede transcurrir antes de que se cierre la sesión interactiva inactiva de un usuario.

Procedimiento

1. Haga clic en **Administrar** desde el inventario de VMware Host Client y, a continuación, haga clic en **Configuración avanzada**.

2 Introduzca **`UserVars.ESXiShellInteractiveTimeOut`** en el cuadro de texto **Buscar** y haga clic en el icono **Buscar**.

3 Haga clic con el botón secundario en `UserVars.ESXiShellInteractiveTimeOut` y seleccione **Editar opción** en el menú desplegable.

   Se abrirá entonces el cuadro de diálogo **Editar opción**.

4 En el cuadro de texto **Nuevo valor**, introduzca la configuración de tiempo de espera.

   Un valor de cero (0) deshabilita el tiempo de inactividad.

5 Haga clic en **Guardar**.

   El tiempo de espera solo se aplica a las sesiones iniciadas recientemente.

6 (opcional) Para restablecer la configuración de clave predeterminada, haga clic con el botón derecho en la clave adecuada de la lista y seleccione **Restablecer al valor predeterminado**.

Resultados

Si la sesión está inactiva, se cerrará la sesión de los usuarios una vez transcurrido el período de tiempo de espera.

Poner un host en modo de mantenimiento en VMware Host Client

Un host se pone en modo de mantenimiento cuando se deben realizar tareas de mantenimiento en él, por ejemplo, para instalar más memoria. El host entra en este modo o sale de él solo mediante la solicitud de un usuario.

El host está en estado **Entrando en modo de mantenimiento** hasta que todas las máquinas virtuales se apagan o migran a otros hosts. No se pueden apagar máquinas virtuales ni migrar máquinas virtuales a un host que está entrando en modo de mantenimiento o que ya se encuentra en dicho modo.

Para poner un host en modo de mantenimiento, todas las máquinas virtuales que están en ejecución en el host deben apagarse o migrarse a hosts diferentes. Si intenta poner en modo de mantenimiento un host que tiene máquinas virtuales en ejecución, DRS deberá apagar o migrar las máquinas virtuales que estén en ejecución para completar la tarea. Si el tiempo de espera se cumple antes de que se apaguen o se migren las máquinas virtuales, aparecerá un mensaje de error.

Cuando todas las máquinas virtuales en el host están inactivas, el icono del host muestra el estado **en mantenimiento** y el panel de resumen del host indica el nuevo estado. Mientras está en modo de mantenimiento, el host no permite implementar ni encender una máquina virtual.

Requisitos previos

Antes de poner un host en modo de mantenimiento, apague todas las máquinas virtuales que se estén ejecutando en ese host o mígrelas hacia otro host, ya sea en forma manual o de manera automática mediante DRS.

Procedimiento

- Haga clic con el botón derecho en el host y seleccione **Entrar en modo de mantenimiento**.

Resultados

El host permanece en modo de mantenimiento hasta que se selecciona **Salir del modo de mantenimiento**.

Administrar permisos en VMware Host Client

En ESXi, los permisos se definen como funciones de acceso que incluyen las funciones que se le asignan a un usuario para diversos objetos, como una máquina virtual o un host ESXi. Los permisos otorgan a los usuarios el derecho de realizar las actividades especificadas por el rol en el objeto al cual se asigna el rol.

Por ejemplo, para configurar la memoria del host, debe otorgarse al usuario una función que incluya el privilegio **Host.Configuración.Configuración de memoria**. Cuando a los usuarios se les asignan distintas funciones para diferentes objetos, se pueden controlar las tareas que estos pueden realizar mientras usan VMware Host Client.

Cuando las cuentas root y vpxuser se conectan directamente a un host con VMware Host Client, tienen los mismos derechos de acceso que cualquier usuario con función de administrador en todos los objetos.

Los demás usuarios, en un principio, no tienen permisos en ningún objeto, lo cual implica que no pueden ver ni realizar tareas en esos objetos. Un usuario con privilegios de administrador debe asignar permisos a estos usuarios para que puedan realizar tareas.

Muchas tareas necesitan permisos en más de un objeto. Las siguientes reglas permiten determinar qué funciones se deben asignar a los usuarios para que realicen determinadas tareas:

- Cualquier tarea que consuma espacio de disco, como la creación de un disco virtual o la captura de una snapshot, necesita el privilegio **Almacén de datos.Asignar espacio** en el almacén de datos de destino, así como el privilegio para realizar la operación en sí.
- Cada host o clúster tiene su propio grupo de recursos implícito, que contiene todos los recursos de ese host o clúster. Para implementar una máquina virtual directamente en un host o un clúster, se necesita el privilegio **Recurso.Asignar máquina virtual a un grupo de recursos**.

La lista de privilegios es la misma para ESXi y vCenter Server.

Se pueden crear roles y establecer permisos a través de una conexión directa al host ESXi.

Validar permisos

Los hosts de vCenter Server y ESXi que usan Active Directory validan regularmente los usuarios y los grupos con el dominio de Windows Active Directory. Esta validación ocurre cada vez que el sistema host se inicia y en intervalos regulares especificados en la configuración de vCenter Server.

Por ejemplo, si al usuario Smith se le asignaron permisos, y en el dominio se modificó el nombre del usuario por Smith2, el host considera que Smith ya no existe y quita los permisos de ese usuario en la siguiente validación.

De modo similar, si se quita el usuario Smith del dominio, todos los permisos se quitan en la siguiente validación. Si se agrega un nuevo usuario Smith al dominio antes de la siguiente validación, el nuevo usuario Smith recibe todos los permisos que se habían asignado al usuario Smith anterior.

Asignar permisos a un usuario para un host ESXi en VMware Host Client

Para poder realizar actividades específicas en un host ESXi, el usuario debe tener permisos asociados a una función en particular. En VMware Host Client, puede asignar funciones a los usuarios y otorgarles los permisos necesarios para realizar diversas tareas en el host.

Procedimiento

1 Haga clic con el botón secundario en **Host** en el inventario de VMware Host Client y, a continuación, haga clic en **Permisos**.

2 Haga clic en **Agregar usuario**.

3 Haga clic en la flecha junto al cuadro de texto **Seleccionar un usuario** y seleccione el usuario al que desea asignar una función.

4 Haga clic en la flecha junto al cuadro de texto **Seleccionar una función** y seleccione una función de la lista.

5 (opcional) Seleccione **Propagar a todos los objetos secundarios** o **Agregar como grupo**.

   Si define un permiso en un nivel de vCenter Server y lo propaga a los objetos secundarios, el permiso se aplica a centros de datos, carpetas, clústeres, hosts, máquinas virtuales y otros objetos de la instancia de vCenter Server.

6 Haga clic en **Agregar** y luego en **Cerrar**.

Quitar permisos para un usuario en VMware Host Client

Si se le quita un permiso a un usuario, no se elimina a ese usuario de la lista de usuarios disponibles. Además, tampoco se quita el rol en la lista de elementos disponibles. Sin embargo, se quita al par usuario-rol en el objeto de inventario seleccionado.

Procedimiento

1 Haga clic con el botón secundario en **Host** en el inventario de VMware Host Client y, a continuación, haga clic en **Permisos**.

2 Seleccione un usuario de la lista y haga clic en **Quitar usuario**.

3 Haga clic en **Cerrar**.

Asignar a un usuario permisos para una máquina virtual en VMware Host Client

Asigne a un usuario en particular una función que le otorgue permisos para realizar tareas específicas en una máquina virtual.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Haga clic con el botón secundario en una máquina virtual de la lista y seleccione **Permisos**.

3 Haga clic en **Agregar usuario**.

4 Haga clic en la flecha junto al cuadro de texto **Seleccionar un usuario** y seleccione el usuario al que desea asignar una función.

5 Haga clic en la flecha junto al cuadro de texto **Seleccionar una función** y seleccione una función de la lista.

6 (opcional) Seleccione **Propagar a todos los objetos secundarios**.

Si define un permiso en un nivel de vCenter Server y lo propaga a los objetos secundarios, el permiso se aplica a centros de datos, carpetas, clústeres, hosts, máquinas virtuales y objetos similares de la instancia de vCenter Server.

7 Haga clic en **Agregar** y luego en **Cerrar**.

Quitar permisos para una máquina virtual en VMware Host Client

Para que un usuario ya no pueda realizar tareas en una máquina virtual en particular, debe quitar los permisos de ese usuario para esa máquina virtual.

Al quitar un permiso a un usuario, este no se elimina de la lista de usuarios disponibles. Además, tampoco se quita el rol en la lista de elementos disponibles. Sin embargo, se quita al par usuario-rol en el objeto de inventario seleccionado.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Haga clic con el botón secundario en una máquina virtual de la lista y seleccione **Permisos**.

3 Seleccione un usuario de la lista y haga clic en **Quitar usuario**.

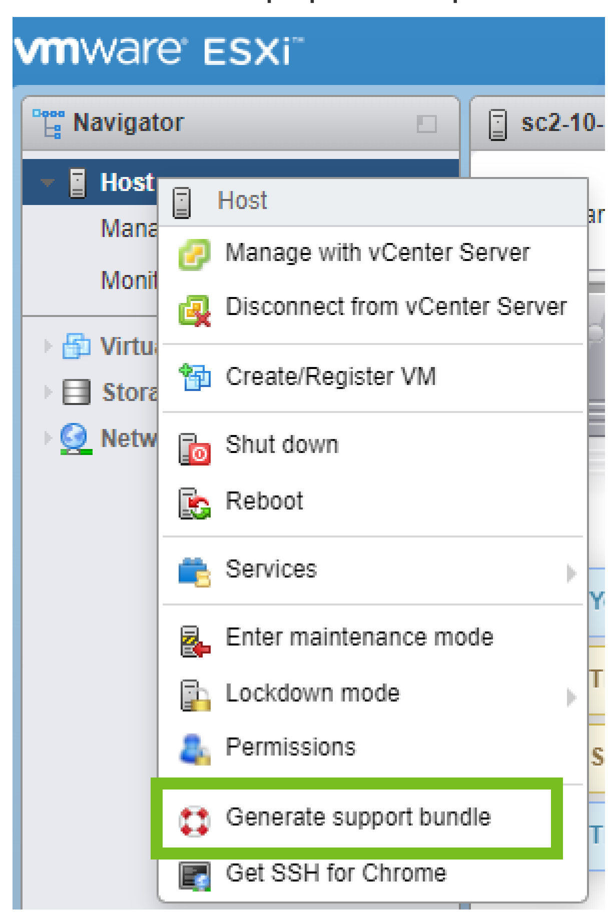
4 Haga clic en **Cerrar**.

Generar un paquete de soporte en VMware Host Client

Puede generar un paquete de soporte para el host ESXi en el que ha iniciado sesión. El paquete de soporte contiene archivos de registro e información del sistema que puede usar para diagnosticar y solucionar problemas.

Procedimiento

1 Haga clic con el botón derecho en **Host** desde el inventario de VMware Host Client y seleccione **Generar paquete de soporte** en el menú desplegable.



Cuando se crea un paquete de soporte, aparece un cuadro de diálogo que contiene un vínculo para descargar el paquete.

2 (opcional) Haga clic en **Supervisar** en el inventario de VMware Host Client, luego en **Tareas** y, a continuación, en un paquete registrado de la lista.

Puede ver el vínculo del paquete de registro en la tabla.

Modo de bloqueo

Para mejorar la seguridad de los hosts ESXi, puede ponerlos en modo de bloqueo. En el modo de bloqueo, las operaciones deben realizarse mediante vCenter Server de forma predeterminada.

Modo de bloqueo normal y modo de bloqueo estricto

Con vSphere 6.0 y las versiones posteriores, se puede seleccionar el modo de bloqueo normal o el modo de bloqueo estricto.

Modo de bloqueo normal

En el modo de bloqueo normal, el servicio de la DCUI permanece activo. Si se pierde la conexión con el sistema vCenter Server y el acceso a través de vSphere Client deja de estar disponible, las cuentas con privilegios pueden iniciar sesión en la interfaz de la consola directa del host ESXi y salir del modo de bloqueo. Solo las siguientes cuentas pueden acceder a la interfaz de usuario de la consola directa:

- Cuentas de la lista de usuarios con excepción para el modo de bloqueo que tienen privilegios administrativos en el host. La lista de usuarios con excepción está pensada para las cuentas de servicio que realizan tareas específicas. Al agregar administradores de ESXi a esta lista, se anula el propósito del modo de bloqueo.
- Usuarios definidos en la opción avanzada DCUI.Access del host. Esta opción sirve para tener acceso de emergencia a la interfaz de la consola directa en caso de que se pierda la conexión con vCenter Server. Estos usuarios no necesitan privilegios administrativos en el host.

Modo de bloqueo estricto

En el modo de bloqueo estricto, el servicio de la DCUI se interrumpe. Si se pierde la conexión con vCenter Server y vSphere Client deja de estar disponible, el host ESXi deja de estar disponible, a menos que se habiliten los servicios ESXi Shell y SSH, y se definan usuarios con excepción. Si no es posible restaurar la conexión con el sistema vCenter Server, debe reinstalar el host.

Modo de bloqueo y servicios ESXi Shell y SSH

El modo de bloqueo estricto interrumpe el servicio de la DCUI. Sin embargo, los servicios ESXi Shell y SSH son independientes del modo de bloqueo. Para que el modo de bloqueo sea una medida de seguridad efectiva, asegúrese de que los servicios ESXi Shell y SSH también estén deshabilitados. Estos servicios están deshabilitados de forma predeterminada.

Cuando un host está en modo de bloqueo, los usuarios que están en la lista de usuarios con excepción pueden acceder a él desde ESXi Shell y a través de SSH si cuentan con el rol de administrador en el host. Se puede tener este tipo de acceso incluso en el modo de bloqueo estricto. La opción más segura es dejar los servicios ESXi Shell y SSH deshabilitados.

Nota La lista de usuarios con excepción no está pensada para administradores, sino para las cuentas de servicio que realizan tareas específicas, como copias de servicio de hosts. Agregar usuarios administradores a la lista de usuarios con excepción va en contra de la finalidad del modo de bloqueo.

Poner un host ESXi en modo de bloqueo normal mediante VMware Host Client

Puede usar VMware Host Client para ingresar al modo de bloqueo normal.

Procedimiento

1 Haga clic en **Host** desde el inventario de VMware Host Client, seleccione **Modo de bloqueo** en el menú desplegable y, a continuación, seleccione **Entrar en bloqueo normal**.

   Aparecerá un mensaje de advertencia.

2 Haga clic en **Entrar en bloqueo normal**.

Poner un host ESXi en modo de bloqueo estricto mediante VMware Host Client

Puede usar VMware Host Client para ingresar al modo de bloqueo estricto.

Procedimiento

1 Haga clic en **Host** desde el inventario de VMware Host Client, seleccione **Modo de bloqueo** en el menú desplegable y, a continuación, seleccione **Entrar en bloqueo estricto**.

   Aparecerá un mensaje de advertencia.

2 Haga clic en **Entrar en bloqueo estricto**.

Salir del modo de bloqueo mediante VMware Host Client

Si ha ingresado en modo de bloqueo normal o estricto en un host ESXi, puede usar VMware Host Client para salir del bloqueo.

Procedimiento

◆ Haga clic en **Host** desde el inventario de VMware Host Client, seleccione **Modo de bloqueo** en el menú desplegable y, a continuación, seleccione **Entrar en bloqueo**.

Especificar usuarios con excepción para el modo de bloqueo en VMware Host Client

En vSphere 6.0 y versiones posteriores, se pueden agregar usuarios a la lista de usuarios con excepción mediante VMware Host Client. Estos usuarios no pierden sus permisos cuando el host entra en el modo de bloqueo. Puede agregar cuentas de servicio, como un agente de copia de seguridad, a la lista de usuarios con excepción.

Los usuarios con excepción son usuarios locales del host o usuarios de Active Directory con privilegios definidos localmente para el host ESXi. No son miembros de un grupo de Active Directory y no son usuarios de vCenter Server. Estos usuarios tienen permitido realizar operaciones en el host en función de sus privilegios. Esto significa que, por ejemplo, un usuario con privilegios de solo lectura no puede deshabilitar el modo de bloqueo en un host.

Nota La lista de usuarios con excepción es útil para las cuentas de servicio que realizan tareas específicas, como copias de servicio de hosts, pero no para los administradores. Agregar usuarios administradores a la lista de usuarios con excepción va en contra de la finalidad del modo de bloqueo.

Procedimiento

1 Haga clic en **Administrar** desde el inventario de VMware Host Client y, a continuación, haga clic en **Seguridad y usuarios**.

2 Haga clic en **Modo de bloqueo**.

3 Haga clic en **Agregar excepción de usuario**, introduzca el nombre del usuario y haga clic en **Agregar excepción**.

4 (opcional) Seleccione un nombre en la lista de usuarios con excepción, haga clic en **Quitar excepción de usuario** y, a continuación, haga clic en **Confirmar**.

Administrar recursos de la CPU mediante VMware Host Client

Al conectar a un host ESXi mediante VMware Host Client, obtiene acceso a un número limitado de opciones de configuración de administración de recursos.

Ver información del procesador mediante VMware Host Client

En VMware Host Client, puede acceder a información acerca de la configuración de CPU actual del host ESXi en el que ha iniciado sesión.

Procedimiento

1 Haga clic en **Host** desde el inventario de VMware Host Client.

2 Expanda **Hardware** y **CPU**.

Se puede ver información sobre la cantidad y el tipo de procesadores físicos, y la cantidad de procesadores lógicos.

Asignar una máquina virtual a un procesador específico en VMware Host Client

Con la afinidad de CPU, puede asignar una máquina virtual a un procesador específico. De esta forma, puede asignar una máquina virtual solamente a un procesador específico disponible en los sistemas con multiprocesador.

Requisitos previos

Apague la máquina virtual.

Procedimiento

1 Haga clic con el botón derecho en una máquina virtual desde el inventario de VMware Host Client y seleccione **Editar configuración**.

2 En **Hardware virtual**, expanda la opción **CPU**.

3 En **Afinidad de programación**, seleccione la afinidad de procesador físico para la máquina virtual.

   Use un guión para indicar los rangos y una coma para separar los valores.

   Por ejemplo, `0, 2, 4-7` indicaría los procesadores 0, 2, 4, 5, 6 y 7.

4 Haga clic en **Guardar** para aplicar los cambios.

Supervisar un host ESXi en VMware Host Client

Al conectarse a un host mediante VMware Host Client, puede supervisar el estado de mantenimiento del host y ver gráficos de rendimiento, eventos, tareas, registros del sistema y notificaciones.

Ver gráficos en VMware Host Client

Cuando inicia sesión en VMware Host Client, puede ver información acerca del uso de recurso del host ESXi que está administrando en forma de gráfico de líneas.

Para reducir el consumo de memoria, VMware Host Client solamente incluye estadísticas de la última hora.

Procedimiento

1 Haga clic en **Supervisar** en VMware Host Client y en **Rendimiento**.

2 (opcional) Para ver el uso del host en la última hora, seleccione una opción en el menú desplegable.

   - Para ver el porcentaje de CPU que usó el host durante la última hora, seleccione **CPU**.
   - Para ver el porcentaje de memoria que usó el host durante la última hora, seleccione **Memoria**.
   - Para ver el porcentaje de red que consumió el host durante la última hora, seleccione **Red**.
   - Para ver el uso de disco que consumió el host durante la última hora, seleccione **Disco**.

Supervisar estado de mantenimiento del hardware en VMware Host Client

Al iniciar sesión en VMware Host Client, puede supervisar el estado de mantenimiento del hardware del host ESXi.

Nota El estado de mantenimiento del hardware solamente está disponible cuando el hardware subyacente lo admite.

Procedimiento

1 Haga clic en **Supervisar** desde el inventario de VMware Host Client y, a continuación, haga clic en **Hardware**.
2 Seleccione el tipo de información que desea ver.
3 (opcional) Para filtrar la lista, utilice los controles de filtro que se encuentran sobre la lista.
4 (opcional) Para ordenar la lista, haga clic en un encabezado de columna.

Ver eventos en VMware Host Client

Los eventos son registros de acciones del usuario o acciones del sistema que se producen en un host ESXi. Al iniciar sesión en VMware Host Client, puede ver todos los eventos asociados con el host que está administrando.

Requisitos previos

Privilegio necesario: **Solo lectura**.

Procedimiento

- Haga clic en **Supervisa** desde el inventario de VMware Host Client y, a continuación, haga clic en **Eventos**.
  a (opcional) Seleccione un evento para ver sus detalles.
  b (opcional) Para filtrar la lista, utilice los controles de filtro que se encuentran sobre la lista.
  c (opcional) Para ordenar la lista, haga clic en un encabezado de columna.

Ver tareas en VMware Host Client

Al iniciar sesión en VMware Host Client, puede ver las tareas que están relacionadas con el host ESXi. Puede ver información acerca del iniciador de las tareas, el estado de las tareas, el resultado de las tareas, la descripción de las tareas, etc.

Procedimiento

- Haga clic en **Supervisar** desde el inventario de VMware Host Client y, a continuación, haga clic en **Tareas**.

  a (opcional) Seleccione una tarea para ver sus detalles.

  b (opcional) Para filtrar la lista, utilice los controles de filtro que se encuentran sobre la lista.

  c (opcional) Para ordenar la lista, haga clic en un encabezado de columna.

Ver registros del sistema en VMware Host Client

Al iniciar sesión en un host ESXi con VMware Host Client, puede ver las entradas de registro para obtener información como quién generó un evento, cuándo se creó el evento y qué tipo de evento es.

Procedimiento

1 Haga clic en **Supervisar** desde el inventario de VMware Host Client y, a continuación, haga clic en **Registros**.

  Se muestra la lista de registros.

2 (opcional) Haga clic en un registro para ver sus detalles.

3 (opcional) Haga clic con el botón derecho en el registro y seleccione una de las opciones siguientes:

  - **Abrir en una ventana nueva**
  - **Generar paquete de soporte**

Ver notificaciones en VMware Host Client

Al iniciar sesión en VMware Host Client, puede ver notificaciones de host y recomendaciones de tareas relacionadas que debe realizar.

Procedimiento

1 Haga clic en **Supervisar** desde el inventario de VMware Host Client y, a continuación, haga clic en **Notificaciones**.

2 Seleccione una notificación de la lista para ver la acción recomendada.

  Se muestra un mensaje con una acción recomendada y una descripción en la lista de notificaciones.

Administrar máquinas virtuales con VMware Host Client

3

Las máquinas virtuales pueden configurarse como equipos físicos y pueden realizar las mismas tareas que estos. Además, las máquinas virtuales son compatibles con características especiales que los equipos físicos no admiten.

Pude usar VMware Host Client para crear, registrar y administrar máquinas virtuales, así como para llevar a cabo tareas administrativas y de solución de problemas que ocurren a diario.

Este capítulo incluye los siguientes temas:

Crear una máquina virtual en VMware Host Client

Las máquinas virtuales son los componentes clave de una infraestructura virtual. Es posible crear máquinas virtuales para agregarlas al inventario del host. Al crear una máquina virtual, se la asocia a un almacén de datos específico, y se seleccionan un sistema operativo y las opciones de hardware virtual. Una vez que la máquina virtual está encendida, esta puede consumir recursos dinámicamente mientras la carga de trabajo aumenta, o bien puede devolver recursos dinámicamente mientras la carga de trabajo disminuye.

Toda máquina virtual tiene dispositivos virtuales que proporcionan la misma función que el hardware físico. Una máquina virtual obtiene CPU y memoria, acceso al almacenamiento y conectividad de red del host en el cual se ejecuta.

Requisitos previos

Verifique si posee los privilegios **Máquina virtual.Inventario.Crear**.

Según las propiedades de la máquina virtual que desee crear, es posible que necesite los siguientes privilegios adicionales:

- **VirtualMachine.Config.AddExistingDisk** si se incluye un dispositivo de disco virtual que hace referencia a un archivo de disco virtual existente (no RDM).
- **VirtualMachine.Config.AddNewDisk** si se incluye un dispositivo de disco virtual que crea un archivo de disco virtual existente (no RDM).
- **VirtualMachine.Config.RawDevice** si se incluye una asignación de dispositivos sin formato (RDM) o un dispositivo de acceso directo a SCSI.
- **VirtualMachine.Config.HostUSBDevice** si se incluye un dispositivo USB virtual, con una copia de seguridad creada por un dispositivo USB de host.
- **VirtualMachine.Config.AdvancedConfig** si se configuran valores en `ConfigSpec.extraConfig`.
- **VirtualMachine.Config.SwapPlacement** si se configura el parámetro swapPlacement.
- **Datastore.AllocateSpace** requerido en todos los almacenes de datos en los que se crean las máquinas virtuales y sus discos virtuales.
- **Network.Assign** requerido en la red que se asigna a la nueva máquina virtual que se va a crear.

Procedimiento

1. Haga clic con el botón derecho en **Host** desde el inventario de VMware Host Client y seleccione **Crear/Registrar máquina virtual**.

   Se abre el asistente **Nueva máquina virtual**.
2. Seleccione **Crear una nueva máquina virtual** y haga clic en **Siguiente**.
3. En la página **Seleccione un nombre y un sistema operativo invitado**, escriba un nombre único para la máquina virtual y configure el sistema operativo invitado.
   a. En el cuadro de texto **Nombre**, introduzca el nombre de la máquina virtual.
   b. En el menú desplegable **Compatibilidad**, seleccione la compatibilidad de la máquina virtual.
   c. En el menú desplegable **Familia del sistema operativo invitado**, seleccione el sistema operativo invitado.

d En el menú desplegable **Versión del sistema operativo invitado**, seleccione la versión del sistema operativo invitado.

e Para habilitar VBS en la máquina virtual, active la casilla **Habilitar seguridad basada en virtualización de Windows** y haga clic en **Siguiente**.

Nota La opción **Habilitar seguridad basada en virtualización de Windows** solo aparece para las versiones más recientes del sistema operativo Windows, por ejemplo, Windows 10 y Windows Server 2016, y si la compatibilidad de la máquina virtual es ESXi 6.7 y versiones posteriores.

Cuando se habilite esta opción, la virtualización de hardware, la IOMMU, la EFI y el arranque seguro estarán disponibles para el sistema operativo invitado. También debe habilitar **Seguridad basada en virtualización** en el sistema operativo invitado de esta máquina virtual.

4 Haga clic en **Siguiente**.

5 En la página **Seleccionar almacenamiento**, seleccione el tipo de almacenamiento de la máquina virtual y un almacén de datos donde almacenar los archivos de la máquina virtual.

a Para guardar todos los discos y los archivos de configuración de máquina virtual en un almacén de datos estándar, haga clic en el botón **Estándar**.

b Para guardar los discos duros de la máquina virtual en el almacén de datos PMem de host local, haga clic en el botón **Memoria persistente**.

c Seleccione un perfil de host en la lista y haga clic en **Siguiente**.

Nota No puede almacenar los archivos de configuración en un almacén de datos PMem. Si decide usar PMem, debe seleccionar un almacén de datos común para los archivos de configuración de la máquina virtual.

6 En la página **Personalizar configuración**, configure el hardware y las opciones de la máquina virtual, y haga clic en **Siguiente**.

Para obtener más información sobre la configuración de discos virtuales y las opciones de las máquinas virtuales, incluidas las instrucciones para agregar distintos tipos de dispositivos, consulte *Administrar máquinas virtuales de vSphere*.

a En la página **Personalizar configuración**, haga clic en **Hardware virtual** y agregue un nuevo dispositivo de hardware virtual.

- Haga clic en el icono **Agregar disco duro** para agregar un nuevo disco duro virtual.

Nota Puede agregar un disco duro de memoria persistente o estándar a la máquina virtual. El disco duro de memoria persistente se almacena en el almacén de datos PMem de host local.

- Haga clic en el icono **Agregar adaptador de red** para agregar una NIC a la máquina virtual.
- Haga clic en el icono **Agregar otro dispositivo** para elegir otro tipo de dispositivo que desee agregar a la máquina virtual.

Nota Si la máquina virtual usa almacenamiento PMem, los discos duros almacenados en un almacén de datos PMem y los dispositivos NVDIMM que se agregan a la máquina virtual comparten, todos, los mismos recursos PMem. Por lo tanto, debe ajustar el tamaño de los dispositivos recién agregados conforme a la cantidad de PMem disponible para el host. Si alguna parte de la configuración requiere atención, el asistente se lo avisará.

b (opcional) Para ver y configurar los ajustes de un dispositivo, expanda el dispositivo.

Opción	Descripción
CPU	La CPU o el procesador es la parte de un sistema del equipo que lleva a cabo las instrucciones de un programa y es el elemento principal en el desempeño de las funciones del equipo. Las CPU contienen núcleos. La cantidad de CPU virtuales que están disponibles en una máquina virtual depende de la cantidad de CPU con licencia en el host y la cantidad de CPU admitidas por el sistema operativo invitado. Para usar la característica de CPU virtuales de varios núcleos de VMware, deberá cumplir con los requisitos del CLUF del sistema operativo invitado.
Memoria	Puede agregar, cambiar o configurar los recursos o las opciones de memoria de la máquina virtual para mejorar su rendimiento. Puede configurar la mayoría de los parámetros de memoria durante la creación de la máquina virtual o después de instalar el sistema operativo invitado. La configuración de recursos de memoria para una máquina virtual determina cuánta memoria del host se asigna a la máquina virtual. El tamaño de la memoria de hardware virtual determina cuánta memoria hay disponible para las aplicaciones que se ejecutan en la máquina virtual.

Opción	Descripción
Disco duro	Puede agregar discos virtuales de gran capacidad a máquinas virtuales y, asimismo, agregar más espacio a los discos existentes, incluso mientras la máquina virtual está en ejecución. Puede establecer la mayoría de los parámetros de discos virtuales durante la creación de una máquina virtual o después de instalar el sistema operativo invitado.
Controlador SCSI	Las controladoras de almacenamiento se presentan a una máquina virtual como diferentes tipos de controladoras SCSI, incluidas controladoras BusLogic paralelo, LSI Logic paralelo, LSI Logic SAS y VMware Paravirtual SCSI. Puede establecer el tipo de recurso compartido de bus de SCSI para una máquina virtual e indicar si se debe compartir el bus de SCSI. Según el tipo de recurso compartido, las máquinas virtuales pueden acceder al mismo disco virtual simultáneamente en el mismo servidor o en otro servidor. Es posible cambiar la configuración de la controladora SCSI de una máquina virtual solamente en un host ESXi.
Controlador SATA	Si una máquina virtual tiene varios discos duros o dispositivos de CD/ DVD-ROM, puede agregar hasta tres controladoras SATA adicionales para asignar los dispositivos. Al propagar los dispositivos entre varias controladoras, se mejora el rendimiento y se evita la congestión del tráfico de datos. También se pueden agregar controladoras adicionales si se supera el límite de 30 dispositivos para una sola controladora. Es posible arrancar máquinas virtuales desde controladoras SATA y utilizarlas para discos duros virtuales de gran capacidad.
Adaptador de red	Al configurar una máquina virtual, puede agregar adaptadores de red (NIC) y especificar el tipo de adaptador. Los tipos de adaptadores de red que están disponibles dependen de los siguientes factores: ■ La compatibilidad de la máquina virtual, que depende del host que la creó o la actualizó más recientemente. ■ Si se actualizó la compatibilidad de la máquina virtual a la versión más reciente para el host actual. ■ El sistema operativo invitado.
Unidad de CD/DVD	Puede configurar dispositivos de CD o DVD para que se conecten a dispositivos cliente, dispositivos de host o archivos ISO de almacenes de datos.
Tarjeta de vídeo	Puede seleccionar la configuración predeterminada o especificar una configuración personalizada. Puede especificar el número de pantallas, la memoria de vídeo total y habilitar la compatibilidad 3D para sistemas operativos invitados en los que VMware admite 3D.
Dispositivo PCI	Puede configurar dispositivos PCI en un host ESXi para que estén disponibles para el acceso directo. También puede cambiar la etiqueta de hardware para restringir la colocación de la máquina virtual a instancias de hardware específicas.
Dispositivo PCI dinámico	Los dispositivos de acceso directo PCI se agrupan automáticamente por su proveedor y nombre de modelo. Puede configurar los dispositivos deseados según el proveedor y el nombre del modelo en lugar de seleccionar un dispositivo PCI físico según la dirección de hardware. Puede agregar todos los dispositivos disponibles con la misma etiqueta

Opción	Descripción
	de hardware o con una etiqueta de hardware en blanco a una máquina virtual. Cuando se enciende una máquina virtual, los dispositivos de acceso directo PCI físicos específicos cuyo proveedor y nombre de modelo coincidan se asocian a la máquina virtual.
Dispositivos de seguridad	Puede configurar Virtual Software Guard Extensions (vSGX) de Intel® para las máquinas virtuales y proporcionar seguridad adicional a las cargas de trabajo. Puede habilitar o deshabilitar vSGX cuando crea una máquina virtual o edita una máquina virtual existente.

c (opcional) Para eliminar un dispositivo, haga clic en el icono Eliminar ( ) que aparece junto al dispositivo.

Esta opción solo aparece para el hardware virtual que se puede quitar de forma segura.

d (opcional) Para personalizar las opciones de la máquina virtual, haga clic en el botón **Opciones de máquina virtual**.

7 En la página **Listo para completar**, revise los detalles y haga clic en **Finalizar**.

Implementar una máquina virtual a partir de un archivo OVF u OVA en VMware Host Client

Al conectarse a un host ESXi mediante VMware Host Client, puede implementar máquinas virtuales a partir de archivos OVF, VMDK y OVA.

Procedimiento

1 Limitaciones de OVF y OVA para VMware Host Client

Puede crear una máquina virtual en VMware Host Client mediante archivos OVF y VMDK, o mediante archivos OVA. Sin embargo, se aplican varias limitaciones a estos métodos de implementación.

2 Implementar una máquina virtual a partir de un archivo OVF u OVA en VMware Host Client

Use el asistente **Nueva máquina virtual** para implementar máquinas virtuales a partir de archivos OVF, OVA o VMDK.

Limitaciones de OVF y OVA para VMware Host Client

Puede crear una máquina virtual en VMware Host Client mediante archivos OVF y VMDK, o mediante archivos OVA. Sin embargo, se aplican varias limitaciones a estos métodos de implementación.

Limitaciones de OVA

Puede cargar archivos OVA mediante un cliente o un explorador web. Los requisitos de memoria son importantes y pueden hacer que el explorador web no responda o que el sistema se vuelva inestable. El tamaño del archivo OVA que se puede cargar depende de la cantidad de memoria disponible en el sistema. Las pruebas de VMware demuestran que Google Chrome puede cargar archivos OVA de 1 gigabyte. Mozilla Firefox puede extraer archivos OVA más grandes, pero existe la posibilidad de que deje de responder.

Para implementar archivos OVA grandes, VMware recomienda primero extraer el archivo OVA en el sistema ejecutando el comando tar `-xvf <file.ova>`. Después podrá proporcionar los archivos OVF y VMDK como archivos separados al asistente de implementación.

Limitaciones de OVF

El tamaño de los archivos OVF que un explorador web puede cargar también presenta limitaciones. Los diferentes exploradores web presentan distintos límites de tamaño de archivos. Mozilla Firefox tiene un límite de 4 GB. Google Chrome puede manejar archivos más grandes y no posee límites documentados.

Implementar una máquina virtual a partir de un archivo OVF u OVA en VMware Host Client

Use el asistente **Nueva máquina virtual** para implementar máquinas virtuales a partir de archivos OVF, OVA o VMDK.

La implementación de OVA se limita a archivos de menos de 1 GB de tamaño debido a las limitaciones de los exploradores web. Para implementar un archivo OVA de más de 1 GB, extraiga el archivo OVA mediante tar y proporcione los archivos OVF y VMDK por separado.

Procedimiento

1. Haga clic con el botón derecho en **Host** desde el inventario de VMware Host Client y seleccione **Crear/Registrar máquina virtual**.

   Se abre el asistente **Nueva máquina virtual**.

2. En la página **Seleccionar tipo de creación**, seleccione **Implementar una máquina virtual a partir de un archivo OVF u OVA** y haga clic en **Siguiente**.

3. En la página **Seleccione los archivos OVF y VMDK**, proporcione un nombre único para la máquina virtual.

   Nota Los nombres de las máquinas virtuales pueden contener hasta 80 caracteres.

4. Para seleccionar un archivo OVF y VMDK, o un archivo OVA para implementar, haga clic en el panel azul.

   Se abre el almacenamiento de su sistema local.

5 Seleccione el archivo que desee implementar en la máquina virtual y haga clic en **Abrir**.

   El archivo que seleccionó aparece en el panel azul.

6 Haga clic en **Siguiente**.

7 En la página **Seleccionar almacenamiento**, elija el tipo de almacenamiento para la máquina virtual.

   a Para guardar todos los discos y los archivos de configuración de máquina virtual en un almacén de datos estándar, haga clic en el botón **Estándar**.

   b Para guardar los discos duros de la máquina virtual en el almacén de datos PMem de host local, haga clic en el botón **Memoria persistente**.

   c Seleccione un perfil de host en la lista y haga clic en **Siguiente**.

   Importante Los archivos de configuración no se pueden guardar en un almacén de datos PMem. Si decide usar PMem, debe seleccionar un almacén de datos común para los archivos de configuración de la máquina virtual.

8 En la página **Opciones de implementación**, seleccione las asignaciones de red, el aprovisionamiento de disco y si desea que la máquina virtual se encienda después de la implementación.

9 Haga clic en **Siguiente**.

10 En la página **Listo para completar**, revise los detalles y haga clic en **Finalizar**.

Resultados

La máquina virtual aparece en el inventario de VMware Host Client, en **Máquinas virtuales**.

Registrar una máquina virtual existente en VMware Host Client

Si cancela el registro de una máquina virtual desde un host, pero no la elimina del almacén de datos, puede volver a registrarla usando VMware Host Client. Al volver a registrar una máquina virtual, aparece de nuevo en el inventario.

Use el navegador del almacén de datos para seleccionar un almacén de datos, un directorio o un archivo `.vmx` para agregar a la lista de máquinas virtuales que se registran. Al seleccionar un almacén de datos o un directorio, se buscan todos los archivos `.vmx` que se encuentran en esa ubicación. Puede examinar más de una vez para anexar máquinas virtuales a la lista.

Procedimiento

1 Haga clic con el botón derecho en **Host** desde el inventario de VMware Host Client y seleccione **Crear/Registrar máquina virtual**.

   Se abre el asistente **Nueva máquina virtual**.

2 En la página **Seleccionar tipo de creación**, elija **Registrar una máquina virtual existente** y haga clic en **Siguiente**.

3 En la página **Seleccionar máquinas virtuales para registro**, haga clic en **Seleccione una o más máquinas virtuales, un almacén de datos o un directorio**, busque la máquina virtual que desea registrar y haga clic en **Seleccionar**.

4 Para quitar una máquina virtual de la lista, seleccione el nombre del archivo y haga clic en **Quitar lo seleccionado**.

5 Para anular la selección y volver a empezar, haga clic en **Quitar todo**.

6 Haga clic en **Siguiente**.

7 En la página **Listo para completar**, revise los detalles y haga clic en **Finalizar**.

Usar consolas en VMware Host Client

Puede acceder a una máquina virtual mediante una consola del explorador o mediante VMware Remote Console (VMRC) en VMware Host Client y realizar diferentes tareas en la máquina virtual.

Usar consolas del explorador

Nota La consola del explorador no es compatible con ninguna versión de ESXi anterior a la 6.0. Debe usar VMRC para acceder a la consola del explorador.

Puede usar una consola del explorador para obtener acceso al sistema operativo invitado sin instalar software adicional. Para obtener funcionalidades de consola adicionales, como conectar hardware local, instale VMware Remote Console.

Nota Actualmente, las consolas de explorador solo admiten la distribución del teclado estadounidense, japonesa y alemana. Debe seleccionar la distribución del teclado deseada antes de abrir la consola.

Usar VMware Remote Console

VMware Remote Console proporciona acceso a máquinas virtuales en hosts remotos y realiza operaciones en consolas y dispositivos, como la configuración de opciones del sistema operativo y la supervisión de la consola de máquinas virtuales para *VMware vSphere*. Puede realizar varias tareas en la máquina virtual, como reiniciar y apagar el sistema operativo invitado de la máquina virtual, reanudar y suspender la máquina virtual, configurar las actualizaciones de VMware Tools, configurar y administrar la máquina virtual y diferentes dispositivos, etc. VMRC también puede modificar la configuración de las máquinas virtuales, como la RAM, los núcleos de CPU y los discos. VMware Workstation™, VMware Fusion™ o VMware Player™ funcionan como clientes de VMRC, de modo que no es necesario descargar e instalar VMRC si cualquiera de los tres está instalado en el sistema.

Para obtener un conjunto completo de funciones de consola, puede descargar e instalar VMRC.

Instalar la aplicación VMware Remote Console en el VMware Host Client

VMware Remote Console (VMRC) es una aplicación de consola independiente que permite conectarse a dispositivos cliente y ejecutar las consolas de máquinas virtuales en hosts remotos.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

  Se mostrará la lista de máquinas virtuales disponibles en el host.

2 Seleccione una máquina virtual de la lista.

3 Haga clic en el icono **Consola** de la barra de herramientas y seleccione la opción **Descargar VMRC**.

Iniciar Remote Console para una máquina virtual en VMware Host Client

Puede acceder a máquinas virtuales en VMware Host Client mediante VMware Remote Console. Puede iniciar una consola o más para acceder a varias máquinas virtuales remotas al mismo tiempo.

Requisitos previos

Compruebe que VMware Remote Console esté instalada en su sistema local.

Procedimiento

1 Haga clic en **Máquinas virtuales** desde el inventario de VMware Host Client y, a continuación, seleccione una máquina virtual de la lista.

2 Haga clic en **Consola** y seleccione **Iniciar Remote Console** en el menú desplegable.

  VMware Remote Console se abre como aplicación independiente para la máquina virtual seleccionada.

Abrir la consola de una máquina virtual en VMware Host Client

Con VMware Host Client, puede acceder al escritorio de una máquina virtual mediante la ejecución de una consola en la máquina virtual. Desde la consola, puede realizar tareas en la máquina virtual, como configurar opciones del sistema operativo, ejecutar aplicaciones, supervisar el rendimiento, etc.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Haga clic en una máquina virtual encendida de la lista.

3 Haga clic en el icono **Consola** de la barra de herramientas y seleccione si desea abrir la consola en una ventana emergente, una nueva ventana o una nueva pestaña.

Administrar un sistema operativo invitado en VMware Host Client

Con VMware Host Client, puede administrar el sistema operativo invitado de la máquina virtual. Puede instalar y actualizar VMware Tools, además de apagar, reiniciar y cambiar el sistema operativo invitado configurado.

Apagar y reiniciar un sistema operativo invitado mediante VMware Host Client

Instale VMware Tools en una máquina virtual para poder apagar y reiniciar el sistema operativo invitado en esa máquina virtual.

Procedimiento

- Haga clic en **Máquinas virtuales** en el inventario VMware Host Client, seleccione una máquina virtual y elija la tarea.
  - Para apagar una máquina virtual, haga clic con el botón derecho en la máquina virtual y seleccione **Sistema operativo invitado > Apagar**.
  - Para reiniciar una máquina virtual, haga clic con el botón derecho en la máquina virtual y seleccione **Sistema operativo invitado > Reiniciar**.

Cambiar el sistema operativo invitado en VMware Host Client

Para cambiar el tipo de sistema operativo invitado en la configuración de máquina virtual, debe modificar la configuración del sistema operativo invitado en el archivo de configuración de la máquina virtual. Si desea cambiar el sistema operativo invitado en sí, debe instalar el nuevo sistema operativo en la máquina virtual.

Cuando se configura el tipo de sistema operativo invitado para una nueva máquina virtual, vCenter Server aplica los valores predeterminados de configuración en función del tipo de invitado. Cambiar la configuración del tipo de sistema operativo invitado afecta los rangos y las recomendaciones disponibles en la configuración de la máquina virtual.

Requisitos previos

Apague la máquina virtual.

Procedimiento

1 En el inventario de VMware Host Client, haga clic con el botón derecho en la máquina virtual y seleccione **Editar configuración**.

2 Haga clic en la pestaña **Opciones de máquina virtual** y expanda **Opciones generales**.

3 Seleccione un tipo y una versión de sistema operativo invitado.

   Si selecciona una versión de sistema operativo Windows que admite VBS y si la compatibilidad de la máquina virtual es ESXi 6.7 y versiones posteriores, se muestra la fila VBS en la pestaña **Opciones de máquina virtual**.

4 (opcional) Haga clic en **Habilitar la seguridad basada en virtualización** para habilitar VBS.

   Importante Al habilitar VBS, se requiere el uso de EFI para arrancar la máquina virtual. Un cambio de firmware puede causar que el sistema operativo invitado no arranque.

5 Haga clic en **Guardar** para aplicar los cambios.

Resultados

Los parámetros de configuración de máquina virtual para el sistema operativo invitado se cambian. Ahora puede instalar el sistema operativo invitado.

Introducción a VMware Tools

VMware Tools es un conjunto de servicios y módulos que permiten varias funciones en los productos de VMware para conseguir una mejor administración de los sistemas operativos invitados, así como una interacción fluida con ellos.

VMware Tools tiene la capacidad de:

- Trasmitir mensajes del sistema operativo del host al sistema operativo invitado.
- Personalizar los sistemas operativos invitados como parte de vCenter Server y de otros productos de VMware.
- Ejecutar scripts que ayudan a automatizar las operaciones del sistema operativo invitado. Los scripts se ejecutan cuando cambia el estado de encendido de la máquina virtual.
- Sincronizar la hora del sistema operativo invitado con la hora del sistema operativo host

La administración del ciclo de vida de VMware Tools ofrece un enfoque escalable y simplificado para la instalación y la actualización de VMware Tools. Incluye una serie de funciones mejoradas, mejoras relacionadas con los controladores y compatibilidad con nuevos sistemas operativos invitados.

Debe ejecutar la última versión de VMware Tools o utilice open-vm-tools distribuidos con la distribución del SO de Linux. Si bien un sistema operativo invitado puede ejecutarse sin VMware Tools, siempre debe ejecutar la última versión de VMware Tools en sus sistemas operativos invitados para acceder a las últimas funciones y actualizaciones.

Puede configurar su máquina virtual para comprobar y aplicar automáticamente actualizaciones de VMware Tools cada vez que la encienda.

Para obtener más información sobre cómo habilitar la actualización automática de VMware Tools en sus máquinas virtuales, consulte la *Guía de administración de la máquina virtual vSphere*.

Instalar VMware Tools

Aunque es posible usar un sistema operativo invitado sin VMware Tools, muchas características de VMware solo están disponibles cuando se instala VMware Tools. VMware Tools mejora el rendimiento del sistema operativo invitado de las máquinas virtuales.

La instalación de VMware Tools es parte del proceso de crear nuevas máquinas virtuales. Es importante actualizar VMware Tools cuando haya actualizaciones disponibles. Para obtener información sobre la creación de máquinas virtuales, consulte la *Guía del usuario de VMware Tools*.

Los instaladores de VMware Tools son archivos de imagen ISO. Una imagen ISO es igual que un CD-ROM para su sistema operativo invitado. Cada tipo de sistema operativo invitado, incluido Windows, Linux, Solaris, FreeBSD y NetWare, posee un archivo de imagen ISO. Cuando se instala o se actualiza VMware Tools, la primera unidad de disco CD-ROM virtual de la máquina virtual se conecta de forma temporal al archivo ISO de VMware Tools del sistema operativo invitado.

Para obtener información acerca de la instalación o la actualización de VMware Tools en máquinas virtuales de Windows, Linux, Mac OS X, Solaris, NetWare o FreeBSD, consulte la *Guía del usuario de VMware Tools*.

Instalar VMware Tools desde el VMware Host Client

VMware Tools es un conjunto de utilidades que se instala en el sistema operativo de una máquina virtual. VMware Tools mejora el rendimiento y la administración de la máquina virtual.

Puede instalar VMware Tools en una o más máquinas virtuales mediante el VMware Host Client.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Seleccione una máquina virtual de la lista.

   La máquina virtual debe estar encendida para poder instalar VMware Tools.

3 Haga clic en **Acciones**, seleccione **Sistema operativo invitado** en el menú desplegable y, a continuación, seleccione **Instalar VMware Tools**.

Actualizar VMware Tools

Puede actualizar VMware Tools manualmente o puede configurar las máquinas virtuales para buscar versiones más recientes de VMware Tools e instalarlas.

El sistema operativo invitado comprueba la versión de VMware Tools cuando se enciende una máquina virtual. La barra de estado de su máquina virtual muestra un mensaje cuando se encuentra disponible una versión nueva.

Para las máquinas virtuales vSphere, cuando la versión instalada de VMware Tools está desactualizada, la barra de estado muestra el mensaje:

```
Hay una versión más reciente de Tools disponible para esta máquina virtual
```

En las máquinas virtuales Windows, puede configurar VMware Tools para notificarle cuando se encuentre disponible una actualización. Si esta opción de notificación está habilitada, el icono de VMware Tools de la barra de tareas de Windows incluye un icono de precaución amarillo cuando se encuentra disponible una actualización de VMware Tools.

Para instalar una actualización de VMware Tools, puede utilizar el mismo procedimiento que utilizó para la instalación de VMware Tools por primera vez. La actualización de VMware Tools implica instalar una versión nueva.

Para los sistemas operativos invitados Windows y Linux, puede configurar la máquina virtual para actualizar VMware Tools de forma automática. A pesar de que la comprobación de la versión se realiza cuando se enciende la máquina virtual, en el caso de los sistemas operativos invitados Windows, la actualización automática se realiza cuando se apaga o reinicia la máquina virtual. La barra de estado muestra el mensaje `Instalando VMware Tools...` cuando una actualización se encuentra en progreso. El procedimiento se describe a continuación.

Nota Al actualizar VMware Tools en sistemas operativos invitados Windows, se instalan automáticamente los controladores de gráficos WDDM. El controlador de gráficos WDDM permite que el modo de suspensión de la configuración de energía del sistema operativo invitado ajuste las opciones de suspensión. Por ejemplo, es posible usar la opción de configuración de modo de suspensión **Cambiar la frecuencia con la que el equipo entra en estado de suspensión** para determinar que el sistema operativo invitado entre automáticamente al modo de suspensión después de cierto tiempo o evitar que el sistema operativo invitado pase automáticamente al modo de suspensión después de estar inactivo por un tiempo.

Para las máquinas virtuales vSphere, puede utilizar uno de los siguientes procesos para actualizar varias máquinas virtuales al mismo tiempo.

- Inicie sesión en vCenter Server, seleccione un host o clúster y, en la pestaña **Máquinas virtuales**, especifique las máquinas virtuales en las que realizará una actualización de VMware Tools.
- Utilice vSphere Lifecycle Manager para realizar una actualización orquestada de máquinas virtuales a nivel de carpeta o centro de datos.

Algunas características de una versión en particular a un producto VMware podrían depender de la instalación o la actualización a la versión de VMware Tools incluida en dicha versión. No es siempre necesaria la actualización a la versión más reciente de VMware Tools. Las versiones más nuevas de VMware Tools son compatibles con varias versiones del host. A fin de evitar actualizaciones innecesarias, evalúe si se requieren características y funciones adicionales en su entorno.

Tabla 3-1. Opciones de compatibilidad de máquinas virtuales

Compatibilidad	Descripción
ESXi 7.0 Update 3 y versiones posteriores	Esta máquina virtual (versión de hardware 19) es compatible con ESXi 7.0 Update 3 y versiones posteriores.
ESXi 7.0 Update 2 y versiones posteriores	Esta máquina virtual (versión de hardware 19) es compatible con ESXi 7.0 Update 2 y versiones posteriores.
ESXi 7.0 Update 1 y versiones posteriores	Esta máquina virtual (versión de hardware 18) es compatible con ESXi 7.0 Update 1 y ESXi 7.0 Update 2.
ESXi 7.0 y versiones posteriores	Esta máquina virtual (versión de hardware 17) es compatible con ESXi 7.0, ESXi 7.0 Update 1 y ESXi 7.0 Update 2.
ESXi 6.7 Update 2 y versiones posteriores	Esta máquina virtual (versión de hardware 15) es compatible con ESXi 6.7 Update 2, ESXi 6.7 Update 3, ESXi 7.0, ESXi 7.0 Update 1 y ESXi 7.0 Update 2.
ESXi 6.7 y versiones posteriores	Esta máquina virtual (versión de hardware 14) es compatible con ESXi 6.7, ESXi 6.7 Update 2, ESXi 6.7 Update 3, ESXi 7.0, ESXi 7.0 Update 1 y ESXi 7.0 Update 2.
ESXi 6.5 y versiones posteriores	Esta máquina virtual (versión de hardware 13) es compatible con ESXi 6.5, ESXi 6.7, ESXi 6.7 Update 2, ESXi 6.7 Update 3, ESXi 7.0, ESXi 7.0 Update 1 y ESXi 7.0 Update 2.
ESXi 6.0 y versiones posteriores	Esta máquina virtual (versión de hardware 11) es compatible con ESXi 6.0, ESXi 6.5, ESXi 6.7, ESXi 6.7 Update 2, ESXi 6.7 Update 3, ESXi 7.0, ESXi 7.0 Update 1 y ESXi 7.0 Update 2.

Para obtener más información, consulte la Guía de compatibilidad de VMware en http://www.vmware.com/resources/compatibility.

Actualizar VMware Tools en VMware Host Client

Puede actualizar VMware Tools en una máquina virtual mediante VMware Host Client.

Requisitos previos

Encienda la máquina virtual.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Seleccione una máquina virtual de la lista.

3 Haga clic en **Acciones**, seleccione **Sistema operativo invitado** en el menú desplegable y, a continuación, seleccione **Actualizar VMware Tools**.

Configurar una máquina virtual en VMware Host Client

Puede agregar o configurar la mayoría de las propiedades de la máquina virtual durante el proceso de creación de una máquina virtual o después de crear la máquina virtual e instalar el sistema operativo invitado.

Se pueden configurar tres tipos de propiedades para las máquinas virtuales.

Hardware

Permite ver la configuración actual de hardware y agregar o quitar hardware.

Opciones

Permite ver y configurar una cantidad de propiedades para las máquinas virtuales, como la interacción de la administración de energía entre el sistema operativo invitado y la máquina virtual, y la configuración de VMware Tools.

Recursos

Permite configurar CPU, orígenes de hiperproceso de CPU, memoria y discos.

Comprobar la versión de hardware de una máquina virtual en VMware Host Client

Puede revisar la versión de hardware de la máquina virtual consultando la página de resumen de la máquina virtual.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Haga clic en una máquina virtual de la lista.

La versión de hardware aparece en el nombre de la máquina virtual.

Cambiar el nombre de una máquina virtual en VMware Host Client

Puede cambiar el nombre de una máquina virtual después de finalizar el proceso de creación. El cambio de nombre no modifica el nombre de ningún archivo de la máquina virtual ni el nombre del directorio donde están ubicados los archivos.

Requisitos previos

Apague la máquina virtual.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Editar configuración** en el menú emergente.

3 Haga clic en **Opciones de máquina virtual**.

4 En el cuadro de texto **Nombre de máquina virtual**, introduzca el nuevo nombre de la máquina virtual.

5 Haga clic en **Guardar**.

Ver la ubicación del archivo de configuración de una máquina virtual en VMware Host Client

Puede ver la ubicación de los archivos de configuración y los archivos de trabajo de una máquina virtual mediante VMware Host Client.

Esta información es útil cuando se configuran sistemas de copia de seguridad.

Requisitos previos

Apague la máquina virtual.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Haga clic con el botón derecho en la máquina virtual y, a continuación, haga clic en **Editar configuración**.

3 Haga clic en la pestaña **Opciones de máquina virtual** y expanda **Opciones generales**.

4 Registre la ubicación de los archivos de configuración y los archivos de trabajo.

5 Haga clic en **Cancelar** para salir de la pantalla.

Configurar los estados de energía de máquinas virtuales en VMware Host Client

El cambio de los estados de energía de las máquinas virtuales es útil cuando se realiza el mantenimiento en el host. Puede usar la configuración predeterminada del sistema para los controles de energía de las máquinas virtuales o bien, puede configurar los controles para que interactúen con el sistema operativo invitado. Por ejemplo, puede configurar el control **Apagar** para apagar la máquina virtual o el sistema operativo invitado.

Puede modificar muchas configuraciones de máquinas virtuales mientras dicha máquina se esté ejecutando, pero es posible que se necesite cambiar el estado de energía de la máquina virtual para algunas configuraciones.

No se puede configurar la acción **Encender** ( ). Esta acción enciende una máquina virtual que está detenida o inicia una máquina virtual y ejecuta un script si la máquina virtual se encuentra suspendida y VMware Tools está instalado y disponible. Si VMware Tools no está instalado, inicia la máquina virtual suspendida y no ejecuta un script.

Requisitos previos

- Asegúrese de que tiene privilegios para realizar la operación de energía prevista en la máquina virtual.
- Para establecer funciones de energía opcionales, instale VMware Tools en la máquina virtual.
- Apague la máquina virtual antes de editar las opciones de VMware Tools.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Editar configuración** en el menú desplegable.

3 En la pestaña **Opciones de máquina virtual**, expanda **VMware Tools**.

4 Seleccione una opción en la máquina virtual para el control **Apagar** ( ) en el menú desplegable.

Opción	Descripción
Apagar	Detiene inmediatamente la máquina virtual. Una acción de apagado desconecta el sistema operativo invitado o la máquina virtual. Un mensaje indica que es posible que el sistema operativo invitado no se haya apagado adecuadamente. Use esta opción de apagado solo cuando sea necesario.
Desconectar invitado	Usa VMware Tools para iniciar un apagado en orden del sistema de la máquina virtual. Las operaciones de energía mediante software solo se permiten si VMware Tools está instalado en el sistema operativo invitado.
Valor predeterminado del sistema	Sigue la configuración del sistema. El valor actual de la configuración del sistema aparece entre paréntesis.

5 Seleccione una opción para el control **Suspender** ( ) en el menú desplegable.

Opción	Descripción
Suspender	Pone en pausa toda la actividad de la máquina virtual. Cuando VMware Tools está instalado y disponible, una acción de Suspender ejecuta un script y suspende la máquina virtual. Si VMware Tools no está instalado, una acción de Suspender suspende la máquina virtual sin ejecutar un script.
Poner invitado en espera	Pone el sistema operativo invitado en modo de espera. Esta opción detiene todos los procesos, pero todos los dispositivos virtuales siguen conectados a la máquina virtual.
Valor predeterminado del sistema	Sigue la configuración del sistema. El valor actual de la configuración del sistema aparece entre paréntesis.

6 Seleccione una opción para el control **Restablecer** () en el menú desplegable.

Opción	Descripción
Reiniciar	Apaga y reinicia el sistema operativo invitado sin apagar la máquina virtual. Si VMware Tools no está instalado, la acción Restablecer restablece la máquina virtual.
Reiniciar invitado	Usa VMware Tools para iniciar un reinicio en orden. Las operaciones de energía mediante software solo se permiten si VMware Tools está instalado en el sistema operativo invitado.
Predeterminado	Sigue la configuración del sistema. El valor actual de la configuración del sistema aparece entre paréntesis.

7 Haga clic en **Guardar**.

Editar los parámetros del archivo de configuración en VMware Host Client

Para solucionar ciertos problemas con su sistema, la documentación de VMware o un representante del soporte técnico de VMware pueden proporcionarle instrucciones para modificar o agregar parámetros de configuración de máquinas virtuales.

Importante Cambiar o agregar parámetros cuando un sistema no tiene problemas puede generar inestabilidad y un menor rendimiento en el sistema.

Se aplican las siguientes condiciones:

- Para cambiar un parámetro, debe cambiar el valor existente para el par palabra clave-valor. Por ejemplo, si el par existente es palabra clave/valor y lo modifica a palabra clave/valor2, la nueva palabra clave es valor2.
- No se puede eliminar una entrada de parámetro de configuración.

Precaución Se debe asignar un valor a las palabras clave de parámetros de configuración. Si no asigna un valor, la palabra clave puede recibir el valor 0, falso o deshabilitado, lo que da como resultado una máquina virtual que no puede encenderse.

Requisitos previos

Apague la máquina virtual.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Editar configuración** en el menú emergente.

3 En la pestaña **Opciones de máquina virtual**, expanda **Opciones avanzadas**.

4 En la fila Parámetros de configuración, haga clic en **Editar configuración**.

   Se abrirá el cuadro de diálogo **Parámetros de configuración**.

5 (opcional) Para agregar un parámetro, haga clic en **Agregar parámetro** y escriba un nombre y un valor para el parámetro.

6 (opcional) Para cambiar un parámetro, escriba un valor nuevo en el cuadro de texto **Valor** de ese parámetro.

7 Haga clic en **Aceptar** para guardar los cambios y salir del cuadro de diálogo **Parámetros de configuración**.

8 Haga clic en **Guardar**.

Configurar el inicio automático para una máquina virtual en VMware Host Client

Ajuste las opciones de inicio automático de una máquina virtual para configurar la máquina virtual para que se inicie antes o después que otras máquinas virtuales del host.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Haga clic con el botón derecho en una máquina virtual de la lista.

3 Seleccione **Inicio automático** en el menú emergente y haga clic en la opción para configurar las opciones de inicio automático para esta máquina virtual.

Opción	Descripción
Aumentar la prioridad	Aumente la prioridad de inicio de esta máquina virtual para que se inicie antes que otras máquinas virtuales.
Disminuir prioridad	Disminuya la prioridad de inicio de esta máquina virtual para que se inicie después que otras máquinas virtuales.

Actualizar la compatibilidad de máquinas virtuales mediante el VMware Host Client

La compatibilidad de la máquina virtual determina el hardware virtual disponible en la máquina virtual, que corresponde al hardware físico disponible en el equipo host. Puede actualizar el nivel de compatibilidad para hacer que una máquina virtual sea compatible con la versión más reciente de ESXi que se ejecuta en el host.

Para obtener información sobre las versiones y la compatibilidad del hardware de la máquina virtual, consulte *Administrar máquinas virtuales de vSphere*.

Requisitos previos

- Cree una copia de seguridad o instantánea de las máquinas virtuales. Consulte Usar instantáneas para administrar máquinas virtuales.

- Actualice VMware Tools. En las máquinas virtuales que ejecutan Microsoft Windows, si actualiza la compatibilidad antes de actualizar VMware Tools, estas podrían perder la configuración de red.
- Compruebe que todos los archivos `.vmdk` estén disponibles en el host ESXi en un almacén de datos VMFS3, VMFS5 o NFS.
- Compruebe que la máquina virtual esté almacenada en almacenes de datos VMFS3, VMFS5 o NFS.
- Compruebe que la configuración de compatibilidad de las máquinas virtuales no se haya establecido como la última versión compatible.
- Determine con qué versiones de ESXi desea que sean compatibles las máquinas virtuales. Consulte *Administrar máquinas virtuales de vSphere*.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Haga clic con el botón derecho en una máquina virtual de la lista y seleccione **Actualizar compatibilidad de máquina virtual** en el menú emergente.

3 Seleccione la última versión compatible y haga clic en **Actualizar**.

Configurar CPU virtual

Se pueden agregar, cambiar o configurar recursos de CPU para mejorar el rendimiento de una máquina virtual. Se puede establecer la mayoría de los parámetros de CPU al crear las máquinas virtuales o después de instalar el sistema operativo invitado. Para algunas acciones deberá apagar la máquina virtual antes de cambiar la configuración.

VMware utiliza la siguiente terminología. Comprender estos términos puede ayudarlo a planificar una estrategia para la asignación de recursos de CPU.

CPU

La CPU, o el procesador, es el componente de un sistema informático que lleva a cabo las tareas necesarias para que las aplicaciones del equipo se ejecuten. La CPU es el elemento principal que realiza las funciones del equipo. Las CPU contienen núcleos.

Socket de la CPU

Un socket de CPU es un conector físico en la placa base de un equipo que se conecta a una CPU física individual. Algunas placas base poseen múltiples sockets y pueden conectar múltiples procesadores de varios núcleos (CPU).

Núcleo

Un núcleo posee una unidad que contiene una memoria caché L1 y unidades funcionales necesarias para ejecutar aplicaciones. Los núcleos pueden ejecutar aplicaciones o subprocesos en forma independiente. Puede haber uno o más núcleos en una única CPU.

Uso compartido de recursos

Los recursos compartidos especifican la prioridad o importancia relativa de una máquina virtual o un grupo de recursos. Si una máquina virtual tiene dos veces más de un tipo de recursos compartidos que de otro, esta tiene derecho a consumir dos veces más ese recurso cuando las dos máquinas virtuales compiten por recursos.

Asignación de recursos

Puede cambiar la configuración de asignación de recursos de la CPU, como recursos compartidos, reserva y límite, cuando la capacidad de los recursos disponible no satisface la demanda. Por ejemplo, si al final del año, la carga de trabajo de contabilidad aumenta, puede incrementar la reserva del grupo de recursos de contabilidad.

vSphere Virtual Symmetric Multiprocessing (Virtual SMP)

Virtual SMP o vSphere Virtual Symmetric Multiprocessing es una característica que permite a una máquina virtual individual tener varios procesadores.

Limitaciones de CPU virtual

La cantidad máxima de CPU virtuales que puede asignar a una máquina virtual es de 768. La cantidad de CPU virtuales depende del número de CPU lógicas en el host y del tipo de sistema operativo invitado instalado en la máquina virtual.

Tenga en cuenta las siguientes limitaciones:

- Una máquina virtual no puede tener más CPU virtuales que la cantidad de núcleos lógicos del host. El número de núcleos lógicos es igual al número de núcleos físicos si el hiperproceso está deshabilitado, o dos veces más si no lo está.
- Si una máquina virtual en ejecución tiene 128 CPU virtuales o menos, no puede usar la adición en caliente para aumentar aún más el número de CPU virtuales. Para cambiar el número de CPU virtuales de manera que supere ese límite, primero debe apagar la máquina virtual. Por el contrario, si una máquina virtual en ejecución ya tiene más de 128 CPU virtuales, puede utilizar la adición en caliente para aumentar hasta 768 el número de CPU virtuales.
- La cantidad máxima de sockets de CPU virtuales que puede tener una máquina virtual es de 128. Si desea configurar una máquina virtual con más de 128 CPU virtuales, debe utilizar CPU virtuales de varios núcleos.
- No todos los sistemas operativos invitados admiten Virtual SMP, y aquellos que lo admiten podrían aceptar menos procesadores de los que hay disponibles en el host. Para obtener más información sobre la admisión de Virtual SMP, consulte la *guía de compatibilidad de VMware*, en http://www.vmware.com/resources/compatibility.
- Los hosts con hiperproceso podrían afectar el rendimiento de la máquina virtual, según cuál sea la carga de trabajo. La práctica recomendada es probar la carga de trabajo para determinar si se debe habilitar o deshabilitar el hiperproceso en los hosts.

Configurar CPU virtuales de varios núcleos

La compatibilidad con CPU virtuales de varios núcleos de VMware permite controlar la cantidad de núcleos por socket virtual en una máquina virtual. Esta capacidad permite que los sistemas operativos con restricciones de sockets aprovechen más los núcleos de CPU del host, lo que a su vez permite mejorar el rendimiento general.

Importante Cuando configura la máquina virtual con las opciones de CPU virtual con varios núcleos, debe asegurarse de que la configuración cumpla con los requisitos de los términos de licencia del sistema operativo invitado.

La utilización de CPU virtuales de varios núcleos puede ser de suma utilidad cuando ejecuta sistemas operativos o aplicaciones que pueden aprovechar solo una cantidad limitada de sockets de CPU.

Puede configurar la compatibilidad de una máquina virtual con ESXi 7.0 Update 1 y versiones posteriores para tener hasta 768 CPU virtuales. Una máquina virtual no puede tener más CPU virtuales que la cantidad real de CPU lógicos presentes en el host. La cantidad de CPU lógicas indica la cantidad de núcleos de procesador físicos o dos veces esa cantidad si se habilita el hiperproceso. Por ejemplo, si un host posee 128 CPU lógicas, puede configurar la máquina virtual para 128 CPU virtuales.

Puede configurar cómo las CPU virtuales se asignan en términos de núcleos y núcleos por socket. Determine la cantidad de núcleos de CPU que desea en la máquina virtual y, a continuación, seleccione la cantidad de núcleos que desea en cada socket, en función de si quiere una CPU de un solo núcleo, una CPU de dos núcleos, una CPU de tres núcleos y así sucesivamente. Su selección determina la cantidad de sockets que posee la máquina virtual.

La cantidad máxima de sockets de CPU virtuales que puede tener una máquina virtual es de 128. Si desea configurar una máquina virtual con más de 128 CPU virtuales, debe utilizar CPU virtuales de varios núcleos.

Para obtener más información sobre las CPU de varios núcleos, consulte la documentación de *Administrar recursos de vSphere*.

Cambiar la cantidad de CPU virtuales en VMware Host Client

Una máquina virtual con compatibilidad con ESXi 7.0 Update 1 y versiones posteriores puede tener hasta 768 CPU virtuales. Puede cambiar la cantidad de CPU virtuales mientras la máquina virtual está apagada. Si está habilitada la adición en caliente de CPU virtuales, puede aumentar la cantidad de CPU virtuales mientras la máquina virtual ser está ejecutando.

La adición de CPU virtuales en caliente se admite para las máquinas virtuales que admiten CPU de varios núcleos y que tienen compatibilidad con ESXi 5.0 y posterior. Cuando la máquina virtual está encendida y la adición en caliente de CPU está habilitada, es posible agregar CPU virtuales en caliente a la máquina virtual en ejecución. Solo puede agregar múltiplos del número de núcleos por socket.

Si una máquina virtual tiene 128 CPU virtuales o menos, no puede usar la adición en caliente para aumentar aún más el número de CPU virtuales. Para cambiar el número de CPU virtuales de manera que supere ese límite, primero debe apagar la máquina virtual. Por el contrario, si una máquina virtual ya tiene más de 128 CPU virtuales, puede utilizar la adición en caliente para aumentar hasta 768 el número de CPU virtuales.

La cantidad máxima de sockets de CPU virtuales que puede tener una máquina virtual es de 128. Si desea configurar una máquina virtual con más de 128 CPU virtuales, debe utilizar CPU virtuales de varios núcleos.

Importante Cuando configura la máquina virtual con las opciones de CPU virtual con varios núcleos, debe asegurarse de que la configuración cumpla con los requisitos de los términos de licencia del sistema operativo invitado.

Requisitos previos

- Si la función de adición de CPU en caliente no está habilitada, apague la máquina virtual antes de agregar CPU virtuales.
- Para agregar CPU de varios núcleos en caliente, compruebe que la máquina virtual sea compatible con ESXi 5.0 o posterior.
- Verifique que posea el privilegio **Máquina virtual.Configuración.Cambiar número de CPU**.

Procedimiento

1. Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.
2. Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Editar configuración** en el menú emergente.
3. En la pestaña **Hardware virtual**, expanda la opción CPU y seleccione la cantidad de núcleos en el menú desplegable **CPU**.
4. Seleccione la cantidad de núcleos por socket en el menú desplegable **Núcleos por socket**.
5. Haga clic en **Guardar**.

Asignar recursos de CPU en VMware Host Client

Para administrar la demanda de carga de trabajo, puede cambiar la cantidad de recursos de CPU asignados a una máquina virtual mediante la configuración de recursos compartidos, reservas y límites.

Una máquina virtual tiene las siguientes opciones definidas por el usuario, las cuales afectan la asignación de recursos de CPU.

Límite

Limita el consumo de tiempo de CPU para una máquina virtual. Este valor se expresa en MHz o GHz.

Reserva

Especifica la asignación mínima garantizada de una máquina virtual. La reserva se expresa en MHz o GHz.

Recursos compartidos

A cada máquina virtual se le conceden recursos compartidos de CPU. Cuantos más recursos compartidos tenga una máquina virtual, más seguido podrá obtener una porción de tiempo de una CPU cuando no hay tiempo de inactividad de CPU. Los recursos compartidos constituyen una métrica relativa para asignar capacidad de CPU.

Requisitos previos

Apague la máquina virtual.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Editar configuración** en el menú emergente.

3 En la pestaña **Hardware virtual**, expanda **CPU** y asigne la capacidad de CPU para la máquina virtual.

Opción	Descripción
Reserva	Asignación de CPU garantizada para esta máquina virtual.
Límite	El límite superior para la asignación de CPU de esta máquina virtual. Seleccione la opción **Ilimitado** para especificar la ausencia de un límite superior.
Recursos compartidos	Recursos compartidos de CPU para esta máquina virtual en relación con el total de la primaria. Las máquinas virtuales del mismo nivel comparten recursos de acuerdo con sus valores de uso compartido relativos limitados por la reserva y el límite. Seleccione las opciones **Bajo**, **Normal** o **Alto**, que especifican los valores de recursos compartidos respectivamente en una relación de 1:2:4. Seleccione **Personalizado** para dar a cada máquina virtual una cantidad específica de recursos compartidos que expresen un peso proporcional.

4 Haga clic en **Guardar**.

Configurar memoria virtual

Puede agregar, cambiar o configurar los recursos o las opciones de memoria de la máquina virtual para mejorar su rendimiento. Puede configurar la mayoría de los parámetros de memoria durante la creación de la máquina virtual o después de instalar el sistema operativo invitado. Para algunas acciones es necesario apagar la máquina virtual antes de cambiar la configuración.

La configuración de recursos de memoria para una máquina virtual determina cuánta memoria del host se asigna a la máquina virtual. El tamaño de la memoria de hardware virtual determina cuánta memoria hay disponible para las aplicaciones que se ejecutan en la máquina virtual. Una máquina virtual no puede beneficiarse de más recursos de memoria que los configurados en su tamaño de memoria de hardware virtual. Los hosts ESXi limitan el uso de recursos de memoria a la cantidad máxima útil para la máquina virtual, de manera que pueda aceptar los valores predeterminados de recursos de memoria ilimitados.

Cambiar la configuración de la memoria

Puede reconfigurar la cantidad de memoria asignada a una máquina virtual para optimizar el rendimiento.

El tamaño mínimo de la memoria es de 4 MB para máquinas virtuales que utilizan firmware del BIOS. Las máquinas virtuales que utilizan firmware de EFI requieren al menos 96 MB de RAM para poder encenderse.

El tamaño de memoria máximo para las máquinas virtuales que usan firmware del BIOS es 24560 GB. Debe usar firmware de EFI para máquinas virtuales con un tamaño de memoria superior a 6128 GB.

El tamaño máximo de memoria de una máquina virtual depende de la memoria física del host ESXi y la configuración de compatibilidad de la máquina virtual.

Si la memoria de la máquina virtual es mayor que el tamaño de la memoria del host, se produce un intercambio, lo que puede tener un grave efecto en el rendimiento de la máquina virtual. El máximo para el mejor rendimiento representa el umbral por encima del cual la memoria física del host ESXi no es suficiente para ejecutar la máquina virtual a su plena velocidad. Este valor varía a medida que cambian las condiciones en el host, por ejemplo, cuando se encienden o se apagan las máquinas virtuales.

El tamaño de la memoria debe ser un múltiplo de 4 MB.

Tabla 3-2. Memoria máxima de la máquina virtual

Introducida en la versión de host	Compatibilidad de máquinas virtuales	Tamaño máximo de la memoria
ESXi 7.0 Update 3	ESXi 7.0 Update 3 y versiones posteriores	24560 GB
ESXi 7.0 Update 2	ESXi 7.0 Update 2 y versiones posteriores	24560 GB
ESXi 7.0 Update 1	ESXi 7.0 Update 1 y versiones posteriores	24560 GB
ESXi 7.0	ESXi 7.0 y versiones posteriores	6128GB
ESXi 6.7 Update 2	ESXi 6.7 Update 2 y versiones posteriores	6128GB
ESXi 6.7	ESXi 6.7 y versiones posteriores	6128GB

Tabla 3-2. Memoria máxima de la máquina virtual (continuación)

Introducida en la versión de host	Compatibilidad de máquinas virtuales	Tamaño máximo de la memoria
ESXi 6.5	ESXi 6.5 y versiones posteriores	6128GB
ESXi 6.0	ESXi 6.0 y versiones posteriores	4080 GB

La versión de host ESXi indica cuándo comenzó la compatibilidad para el mayor tamaño de memoria. Por ejemplo, el tamaño de memoria de una máquina virtual con compatibilidad de ESXi 6.0 y versiones posteriores que se ejecutan en ESXi 6.5 está restringido a 4080 GB.

Requisitos previos

Compruebe si cuenta con el privilegio **Máquina virtual.Configuración.Cambiar memoria** en la máquina virtual.

Procedimiento

1 Haga clic con el botón derecho en una máquina virtual del inventario y seleccione **Editar configuración**.

2 En la pestaña **Hardware virtual**, expanda **Memoria** y modifique la configuración de memoria.

   a En el cuadro de texto **Memoria**, introduzca la cantidad de RAM que desea asignar a la máquina virtual.

   b Seleccione si la memoria se especifica en MB, GB o TB.

3 Haga clic en **Aceptar**.

Asignar recursos de memoria a una máquina virtual en VMware Host Client

Puede cambiar la cantidad de recursos de memoria asignados a una máquina virtual mediante las opciones de configuración de los límites, las reservas y las cuotas. El host determina cuál es la cantidad correcta de memoria RAM física que debe asignarse a las máquinas virtuales en función de estas opciones de configuración. Puede asignar un valor de cuota alto o bajo a una máquina virtual, según su carga y su estado.

Las siguientes opciones de configuración definidas por el usuario afectan la asignación de recursos de memoria de una máquina virtual.

Límite

Establece un límite para el consumo de memoria de una máquina virtual. Este valor se expresa en megabytes.

Reserva

Especifica la asignación mínima garantizada de una máquina virtual. La reserva se expresa en megabytes. Si no se puede cumplir la reserva establecida, la máquina virtual no se encenderá.

Recursos compartidos

A cada máquina virtual se le concede una determinada cantidad de cuotas de memoria. Cuantas más cuotas tenga una máquina virtual, mayor será la proporción de memoria de host que reciba. Las cuotas representan una métrica relativa para la asignación de capacidad de memoria. Para obtener más información acerca de los valores de cuotas, consulte el documento *Administrar recursos de vSphere*.

No es posible asignar a una máquina virtual una reserva que supere la memoria configurada de la máquina virtual. Si se otorga una reserva de gran tamaño a una máquina virtual y se reduce su tamaño de memoria configurado, se reduce la reserva para que coincida con el nuevo tamaño de memoria configurado.

Requisitos previos

Apague la máquina virtual.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Editar configuración** en el menú emergente.

3 En la pestaña **Hardware virtual**, expanda la opción **Memoria** y asigne más capacidad de memoria para la máquina virtual.

Opción	Descripción
Reserva	Asignación de memoria garantizada para esta máquina virtual.
Límite	El límite superior para la asignación de memoria de esta máquina virtual. Seleccione la opción **Ilimitado** para especificar la ausencia de un límite superior.
Recursos compartidos	Los valores **Bajo**, **Normal**, **Alto** y **Personalizado** se comparan con la suma de todos los recursos compartidos de todas las máquinas virtuales en el servidor.

4 Haga clic en **Guardar**.

Cambiar la configuración de adición de memoria en caliente en VMware Host Client

La adición de memoria en caliente puede agregar recursos de memoria a una máquina virtual mientras la máquina virtual está encendida.

La habilitación de la adición de memoria en caliente produce una cierta sobrecarga adicional de la memoria en el host ESXi de la máquina virtual.

Requisitos previos

- Apague la máquina virtual.
- Verifique que la máquina virtual tenga un sistema operativo invitado que admita las funcionalidades de adición de memoria en caliente.

- Compruebe que la máquina virtual sea compatible con ESXi 4.x y posterior.
- Compruebe que VMware Tools esté instalado.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Editar configuración** en el menú emergente.

3 En la pestaña **Hardware virtual**, expanda **Memoria** y habilite **Conexión en caliente de memoria**.

4 Haga clic en **Guardar**.

Agregar un dispositivo NVDIMM a una máquina virtual en VMware Host Client

Agregue un dispositivo NVDIMM virtual a una máquina virtual para que pueda usar memoria del equipo no volátil o persistente. La memoria no volátil (Non-Volatile Memory, NVM) o la memoria persistente (Persistent Memory, PMem) combinan las velocidades altas de transferencia de datos de la memoria volátil con la persistencia y la resistencia del almacenamiento tradicional. El dispositivo NVDIMM virtual es un dispositivo NVM virtual que puede conservar los datos almacenados a través de reinicios o errores de la fuente de alimentación.

Las máquinas virtuales consumen los recursos PMem del host a través de un módulo virtual de memoria en línea dual no volátil (Non-Volatile Dual In-Line Memory Module, NVDIMM) o mediante un disco de memoria persistente virtual.

Para obtener más información acerca de la memoria persistente, consulte Administrar memoria persistente.

Requisitos previos

- Compruebe que el sistema operativo invitado de la máquina virtual sea compatible con PMem.
- Compruebe que la versión de hardware virtual sea 14 o posterior.
- Compruebe que tiene el privilegio **Almacén de datos.Asignar espacio**.
- Compruebe que el host o el clúster en el que reside la máquina virtual tengan recursos PMem disponibles.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Editar configuración** en el menú emergente.

3 En la pestaña **Hardware virtual**, haga clic en **Agregar otro dispositivo** y seleccione **NVDIMM** en el menú desplegable.

   El dispositivo NVDIMM se mostrará en la lista de dispositivos de Hardware virtual. Cada máquina virtual puede tener un máximo de 64 dispositivos NVDIMM.

4 Configure el dispositivo NVDIMM recién agregado.

   a En la lista de dispositivos de Hardware virtual, expanda **Nuevo NVDIMM**.

   b Introduzca el tamaño del nuevo dispositivo NVDIMM.

   Nota Puede cambiar el tamaño del dispositivo NVDIMM más adelante. La máquina virtual debe estar apagada.

   c Seleccione la ubicación de la controladora de NVDIMM o deje el valor predeterminado.

5 Haga clic en **Guardar** para cerrar el asistente.

Configurar máquina virtual de red

Las funciones de red de ESXi posibilitan la comunicación entre máquinas virtuales del mismo host, entre máquinas virtuales de hosts diferentes y entre otras máquinas físicas y virtuales.

Las funciones de red también permiten la administración de hosts ESXi y habilitan la comunicación entre servicios de VMkernel como NFS, iSCSI o vSphere vMotion y la red física. Al configurar la red para una máquina virtual, se seleccionan o cambian un tipo de adaptador o una conexión de red, además de especificarse si la red deberá conectarse cuando se encienda la máquina virtual.

Aspectos básicos del adaptador de red

Al configurar una máquina virtual, puede agregar adaptadores de red (NIC) y especificar el tipo de adaptador.

Tipos de adaptador de red

Los tipos de adaptadores de red que están disponibles dependen de los siguientes factores:

- La compatibilidad de la máquina virtual, que depende del host que la creó o la actualizó más recientemente.
- Si se actualizó la compatibilidad de la máquina virtual a la versión más reciente para el host actual.
- El sistema operativo invitado.

Las NIC compatibles actualmente son diferentes entre un entorno local y VMware Cloud on AWS. Se admiten los siguientes tipos de NIC en una implementación local:

E1000E

Versión emulada de la tarjeta de interfaz de red (NIC) Gigabit Ethernet Intel 82574. E1000E es el adaptador predeterminado para Windows 8 y Windows Server 2012.

E1000

Versión emulada de la tarjeta de interfaz de red (NIC) Gigabit Ethernet Intel 82545EM, con controladores disponibles en la mayoría de los sistemas operativos invitados más nuevos, incluido Windows XP y versiones posteriores y Linux versión 2.4.19 y versiones posteriores.

Flexible

Se identifica como adaptador Vlance cuando se arranca una máquina virtual, pero se inicializa y funciona como adaptador Vlance o VMXNET, según el controlador que lo inicializa. Con VMware Tools instalado, el controlador VMXNET cambia el adaptador Vlance al adaptador VMXNET de rendimiento más alto.

Vlance

Versión emulada de la tarjeta de interfaz de red (NIC) AMD 79C970 PCnet32 LANCE, una tarjeta de interfaz de red (NIC) más antigua de 10 Mbps disponible en sistemas operativos invitados heredados de 32 bits. Una máquina virtual configurada con este adaptador de red puede utilizar su red de forma inmediata.

VMXNET

Optimizada para el rendimiento en una máquina virtual y sin equivalente físico. Debido a que los proveedores de sistemas operativos no proporcionan controladores integrados para esta tarjeta, debe instalar VMware Tools para tener disponible un controlador para el adaptador de red VMXNET.

VMXNET 2 (mejorado)

Basado en el adaptador VMXNET, pero con características de alto rendimiento comúnmente disponibles en redes modernas, como tramas gigantes y descargas de hardware. VMXNET 2 (mejorado) se encuentra solo disponible en algunos sistemas operativos invitados en ESX/ESXi 3.5 y versiones posteriores.

VMXNET 3

Una tarjeta de interfaz de red (NIC) paravirtualizada diseñada para un gran rendimiento. VMXNET 3 proporciona todas las características disponibles en VMXNET 2 y agrega varias funciones nuevas, como la compatibilidad multicola (también denominada Ajuste de escala en lado de recepción en Windows), descargas IPv6 y entrega de interrupciones MSI/MSI-X. VMXNET 3 no está relacionado con VMXNET o VMXNET 2.

PVRDMA

Una tarjeta de interfaz de red (NIC) paravirtualizada que admite el acceso directo a memoria remota (RDMA) entre las máquinas virtuales a través de la API de verbos de OFED. Todas las máquinas virtuales deben tener un dispositivo PVRDMA y deben estar conectadas a Distributed Switch. PVRDMA es compatible con VMware vSphere vMotion y la tecnología de snapshots. Se encuentra disponible en máquinas virtuales con la versión de hardware 13 y el sistema operativo invitado Linux kernel 4.6 y posteriores.

Para obtener información sobre la asignación de un adaptador de red PVRDMA a una máquina virtual, consulte la documentación de *Redes de vSphere*.

Acceso directo SR-IOV

Representación de una función virtual en una tarjeta de interfaz de red (NIC) física con compatibilidad con SR-IOV. La máquina virtual y el adaptador físico intercambian datos sin utilizar el VMkernel como intermediario. Este tipo de adaptador es adecuado para máquinas virtuales donde la latencia podría causar errores o que requieren más recursos de la CPU.

El acceso directo SR-IOV está disponible en ESXi 6.0 y versiones posteriores para los sistemas operativos invitados Red Hat Enterprise Linux 6 y versiones posteriores, y Windows Server 2008 R2 con SP2. Una versión de un sistema operativo podría incluir un controlador VF predeterminado para determinadas tarjetas de interfaz de red (NIC), mientras que en otros deberá descargarlo e instalarlo desde una ubicación suministrada por el proveedor de la tarjeta de interfaz de red (NIC) o del host.

Para obtener información sobre la asignación de un adaptador de red de acceso directo SR-IOV a una máquina virtual, consulte la *Redes de vSphere* documentación.

En lo que respecta a consideraciones de compatibilidad del adaptador de red, consulte la *Guía de compatibilidad de VMware* en http://www.vmware.com/resources/compatibility.

Versiones de hardware virtual de ESXi y adaptadores de red heredados

Los tipos de adaptadores de red predeterminados para todas las máquinas virtuales heredadas dependen de los adaptadores disponibles y compatibles con el sistema operativo invitado y de la versión del hardware virtual en la que se creó la máquina virtual.

Si no se actualiza una máquina virtual para utilizar una versión de hardware virtual, la configuración del adaptador se mantiene sin cambios. Si actualiza la máquina virtual para aprovechar hardware virtual más reciente, la configuración predeterminada del adaptador probablemente cambie para admitir el sistema operativo invitado y el hardware del host actualizado.

Si desea comprobar los adaptadores de red que están disponibles para su sistema operativo invitado compatible para una versión en particular de vSphere ESXi, consulte la *Guía de compatibilidad de VMware* en http://www.vmware.com/resources/compatibility.

Adaptadores de red y máquinas virtuales heredadas

Las máquinas virtuales heredadas son máquinas virtuales que son compatibles con el producto en uso, pero que no corresponden a la versión actual de ese producto. Los tipos de adaptadores de red predeterminados para todas las máquinas virtuales heredadas dependen de los adaptadores disponibles y compatibles con el sistema operativo invitado y de la versión del hardware virtual en la que se creó la máquina virtual.

Si no se realiza una actualización a una máquina virtual para establecer una correspondencia con una actualización a una versión más reciente de un host ESXi, la configuración del adaptador se mantiene sin modificaciones. Si actualiza la máquina virtual para aprovechar hardware virtual más reciente, la configuración predeterminada del adaptador probablemente cambie para admitir el sistema operativo invitado y el hardware del host actualizado.

Si desea comprobar los adaptadores de red que están disponibles para su sistema operativo invitado compatible para una versión en particular de vSphere ESXi, consulte la *Guía de compatibilidad de VMware* en http://www.vmware.com/resources/compatibility.

Cambiar la configuración del adaptador de red virtual en VMware Host Client

Es posible establecer la configuración de la conexión de encendido, la dirección MAC y la conexión de red del adaptador de red virtual de una máquina virtual.

Requisitos previos

Privilegios necesarios:

- **Máquina virtual..Modificar configuración del dispositivo** para editar la dirección MAC y la red.
- **Máquina virtual.Interacción.Conexión de dispositivos** para cambiar **Conectar** y **Conectar al encender**.
- **Red.Asignar red**

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Editar configuración** en el menú emergente.

3 Haga clic en la pestaña **Hardware virtual** y seleccione el adaptador de red (NIC) en la lista de hardware.

4 (opcional) Para conectar la NIC virtual cuando se enciende la máquina virtual, seleccione **Conectar al encender**.

5 (opcional) Seleccione el tipo de adaptador en el menú desplegable **Tipo de adaptador**.

6 Seleccione una opción para la configuración de la dirección MAC.

Opción	Descripción
Automático	vSphere asigna automáticamente una dirección MAC.
Manual	Introduzca la dirección MAC que se va a utilizar.

7 Haga clic en **Guardar**.

Agregar un adaptador de red a una máquina virtual en VMware Host Client

Cuando agregue un adaptador de red (NIC) a una máquina virtual, deberá seleccionar el tipo de adaptador, la conexión de red y si el dispositivo se conectará cuando se encienda la máquina virtual.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Editar configuración** en el menú emergente.

3 Haga clic en la pestaña **Hardware virtual** y, a continuación, en **Agregar adaptador de red**.

4 En el panel Conexión de red, seleccione una red con una etiqueta específica o una red heredada.

5 (opcional) Si desea configurar la NIC virtual para que se conecte cuando se encienda la máquina virtual, seleccione **Conectar al encender**.

6 Haga clic en **Guardar**.

Configurar un disco virtual

Puede agregar discos virtuales de gran capacidad a máquinas virtuales y, asimismo, agregar más espacio a los discos existentes, incluso mientras la máquina virtual está en ejecución. Puede establecer la mayoría de los parámetros de discos virtuales durante la creación de una máquina virtual o después de instalar el sistema operativo invitado.

Puede almacenar los datos de una máquina virtual en un disco virtual nuevo, en un disco virtual existente o en un LUN de SAN asignado. Un disco virtual aparece como un único disco duro para el sistema operativo invitado. El disco virtual está compuesto por uno o más archivos en el sistema de archivos host. Puede copiar o transferir discos virtuales en un mismo host o entre hosts.

Para las máquinas virtuales que se ejecutan en un host ESXi, puede almacenar los datos de las máquinas virtuales directamente en un LUN de SAN, en lugar de almacenarlos en un archivo de disco virtual. Esta opción es útil si ejecuta en las máquinas virtuales aplicaciones que deben detectar las características físicas del dispositivo de almacenamiento. La asignación de un LUN de SAN permite utilizar los comandos de SAN existentes para administrar el almacenamiento en el disco.

Cuando se asigna un LUN a un volumen de VMFS, vCenter Server o el host ESXi crea un archivo de asignación de dispositivos sin formato (RDM) que apunta al LUN sin formato. El encapsulamiento de la información de disco en un archivo permite que vCenter Server o el host ESXi bloqueen el LUN de manera tal que solo una máquina virtual pueda realizar escrituras en él. El archivo tiene una extensión `.vmdk`, pero solamente contiene información de disco que describe la asignación al LUN en el sistema ESXi. Los datos reales se almacenan en el LUN. No se puede implementar una máquina virtual a partir de una plantilla y almacenar sus datos en un LUN. Solo se pueden almacenar sus datos en un archivo de disco virtual.

La cantidad de espacio libre en el almacén de datos cambia constantemente. Asegúrese de dejar suficiente espacio para la creación de máquinas virtuales y demás operaciones de máquinas virtuales, como el crecimiento de archivos dispersos, snapshots, etc. Para revisar la utilización del espacio para el almacén de datos por tipo de archivo, consulte la documentación de *Supervisión y rendimiento de vSphere*.

El aprovisionamiento fino permite crear archivos dispersos con bloques que se asignan en el momento del primer acceso, lo que permite que el almacén de datos se sobreaprovisione. Los archivos dispersos pueden seguir creciendo y llenar el almacén de datos. Si el almacén de datos se queda sin espacio de disco mientras está ejecutándose la máquina virtual, esta puede dejar de funcionar.

Acerca de las directivas de aprovisionamiento de discos virtuales

Cuando realiza ciertas operaciones de administración de máquina virtual, puede especificar una directiva de aprovisionamiento para el archivo de disco virtual. Las operaciones incluyen crear un disco virtual, clonar una máquina virtual a una plantilla o migrar una máquina virtual.

Los almacenes de datos NFS con aceleración de hardware y los almacenes de datos de VMFS admiten las siguientes directivas de aprovisionamiento de discos. En los almacenes de datos NFS que se no admite la aceleración de hardware, solo está disponible el formato fino.

Puede utilizar Storage vMotion o bien Storage vMotion entre hosts para pasar los discos virtuales de un formato a otro.

Puesta a cero lenta con aprovisionamiento grueso

Crea un disco virtual en un formato grueso predeterminado. El espacio necesario para el disco virtual se asigna en el momento en que se crea el disco. Los datos que quedan en el dispositivo físico no se borran durante la creación, sino que se ponen a cero según demanda más adelante, en la primera escritura de la máquina virtual. Las máquinas virtuales no leen datos obsoletos del dispositivo físico.

Puesta a cero rápida con aprovisionamiento grueso

Un tipo de disco virtual grueso que admite características de clúster, como Fault Tolerance. El espacio necesario para el disco virtual se asigna en el momento de la creación. A diferencia del formato de puesta a cero lenta de aprovisionamiento grueso, los datos que quedan en el dispositivo físico se ponen a cero cuando se crea el disco virtual. Es posible que la creación de discos virtuales en este formato demore más que la creación de otros tipos de disco. Aumentar el tamaño de un disco virtual grueso de puesta a cero rápida provoca un considerable tiempo de inactividad para la máquina virtual.

Aprovisionamiento fino

Utilice este formato para ahorrar espacio de almacenamiento. Para el disco fino, aprovisione tanto espacio de almacén de datos como lo requiera el disco, en función del valor que introduzca para el tamaño del disco virtual. Sin embargo, el disco fino comienza siendo pequeño y, al principio, utiliza solo el espacio de almacén de datos que necesita para las operaciones iniciales. Si posteriormente el disco fino necesita más espacio, puede aumentar su tamaño hasta la capacidad máxima y ocupar todo el espacio del almacén de datos aprovisionado para él.

El aprovisionamiento fino es el método más rápido para crear un disco virtual, ya que crea un disco solo con la información del encabezado. No asigna ni pone a cero los bloques de almacenamiento. Los bloques de almacenamiento se asignan y se ponen a cero la primera vez que se accede a ellos.

Nota Si un disco virtual admite soluciones de agrupación en clústeres, como Fault Tolerance, ese disco no debe tener aprovisionamiento fino.

Cambiar la configuración de discos virtuales en VMware Host Client

Si se queda sin espacio en el disco, puede aumentar el tamaño de este. Puede modificar el nodo del dispositivo virtual y el modo de persistencia de la configuración de disco virtual de una máquina virtual.

Requisitos previos

Apague la máquina virtual.

Compruebe que dispone de los siguientes privilegios:

- **Máquina virtual.Configuración.Modificar configuración del dispositivo** en la máquina virtual.
- **Máquina virtual.Configuración.Extender disco virtual** en la máquina virtual.
- **Almacén de datos.Asignar espacio** en el almacén de datos.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Editar configuración** en el menú emergente.

3 En la pestaña **Hardware virtual**, expanda el disco duro para ver todas las opciones del disco.

4 (opcional) Para cambiar el tamaño del disco, escriba un nuevo valor en el cuadro de texto y seleccione las unidades en el menú desplegable.

5 (opcional) Para modificar la forma en que los discos se ven afectados por las instantáneas, seleccione un modo de disco en el menú desplegable **Modo de disco**.

Opción	Descripción
Dependiente	Se incluyen discos dependientes en las snapshots.
Independiente-persistente	Los discos en modo persistente se comportan como los discos convencionales en el equipo físico. Todos los datos que se escriben en un disco en modo persistente se escriben de forma permanente en el disco.
Independiente-no persistente	Los cambios en los discos en modo no persistente se descartan cuando se apaga o se restablece la máquina virtual. Con el modo no persistente, puede reiniciar la máquina virtual con un disco virtual en el mismo estado cada vez. Los cambios en el disco se escriben y se leen desde un archivo de registro de rehacer que se elimina al apagar o restablecer la máquina virtual.

6 Haga clic en **Guardar**.

Agregar un disco duro estándar nuevo a una máquina virtual en VMware Host Client

Puede agregar un disco duro virtual a una máquina virtual existente, o puede agregar un disco duro cuando personalice el hardware de la máquina virtual durante su proceso de creación. Por ejemplo, es posible que necesite proporcionar espacio de disco adicional para una máquina virtual existente con una gran carga de trabajo. Durante la creación de la máquina virtual, sería conveniente agregar un disco duro que esté configurado previamente como disco de arranque.

Requisitos previos

- Compruebe que conoce bien las opciones de configuración y las advertencias para agregar discos duros virtuales. Consulte Configurar un disco virtual.
- Antes de agregar discos de más de 2 TB a una máquina virtual, consulte *Administrar máquinas virtuales de vSphere*.
- Compruebe que posee el privilegio **Máquina virtual.Configuración.Agregar disco nuevo** en el almacén de datos o en la carpeta de destino.

Apague la máquina virtual.

Procedimiento

1. Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.
2. Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Editar configuración** en el menú emergente.
3. (opcional) Para eliminar un disco duro existente, desplace el cursor sobre el disco y haga clic en el icono **Quitar** (**X**).

   El disco se quita de la máquina virtual. Si otras máquinas virtuales comparten el disco, los archivos de disco no se eliminan.
4. En la pestaña **Hardware virtual**, seleccione **Agregar disco duro** y, a continuación, seleccione **Nuevo disco duro estándar** en el menú desplegable.

   El disco duro aparece en la lista de dispositivos de hardware virtual.
5. Expanda **Nuevo disco duro**.
6. (opcional) Introduzca un valor para el tamaño del disco duro y seleccione las unidades en el menú desplegable.
7. Seleccione la ubicación del almacén de datos en el que desee almacenar los archivos de la máquina virtual.

8 Seleccione el formato del disco de la máquina virtual.

Opción	Descripción
Puesta a cero lenta con aprovisionamiento grueso	Crea un disco virtual en un formato grueso predeterminado. El espacio necesario para el disco virtual se asigna durante la creación. Los datos que quedan en el dispositivo físico no se borran durante la creación, sino que se ponen a cero a petición más adelante, en la primera escritura de la máquina virtual.
Puesta a cero rápida con aprovisionamiento grueso	Permite crear un disco grueso que admita características de clúster, como Fault Tolerance. El espacio necesario para el disco virtual se asigna en el momento de la creación. En contraposición con el formato plano, los datos que quedan en el dispositivo físico se ponen a cero durante la creación. Es posible que la creación de discos en este formato demore mucho más que la creación de otros tipos de discos.
Aprovisionamiento fino	Permite usar el formato de aprovisionamiento fino. Al principio, un disco con aprovisionamiento fino utiliza solo el espacio de almacén de datos que necesita inicialmente. Si más adelante el disco fino necesita más espacio, puede aumentar su tamaño hasta la capacidad máxima que tiene asignada.

9 En el menú desplegable **Recursos compartidos**, seleccione un valor para la asignación de uso compartido al disco virtual.

Recursos compartidos es un valor que representa la medición relativa para controlar el ancho de banda del disco. Los valores Bajo, Normal, Alto y Personalizado se comparan con la suma de todos los recursos compartidos de todas las máquinas virtuales en el host.

10 Si seleccionó la opción **Personalizado**, especifique una cantidad de recursos compartidos en el cuadro de texto.

11 En el cuadro **Límite de IOPS**, especifique el límite superior de los recursos de almacenamiento que se deben asignar a la máquina virtual o seleccione la opción **Ilimitado**.

Este valor es el límite superior de las operaciones de E/S por segundo asignado al disco virtual.

12 Acepte el nodo de dispositivo virtual predeterminado o seleccione uno diferente.

En la mayoría de los casos, debe aceptar el nodo de dispositivo virtual predeterminado. Para un disco duro, usar un nodo de dispositivo que no sea el predeterminado hace que sea más fácil controlar el orden de arranque o tener varios tipos de controladoras SCSI. Por ejemplo, sería conveniente arrancar desde una controladora LSI Logic y compartir un disco de datos con otra máquina virtual que usa una controladora Buslogic con uso compartido del bus activado.

13 (opcional) Seleccione un modo del disco.

Opción	Descripción
Dependiente	Se incluyen discos dependientes en las snapshots.
Independiente-persistente	Los discos en modo persistente se comportan como discos de equipos físicos convencionales. Todos los datos que se escriben en un disco en modo persistente se escriben de forma permanente en el disco.
Independiente-no persistente	Los cambios en los discos en modo no persistente se descartan cuando se apaga o se restablece la máquina virtual. El disco virtual vuelve al mismo estado cada vez que se reinicia la máquina virtual. Los cambios en el disco se escriben y se leen desde un archivo de registro de rehacer que se elimina al apagar o restablecer.

14 Haga clic en **Guardar**.

Agregar un disco duro existente a una máquina virtual en VMware Host Client

Puede agregar un disco duro virtual existente a una máquina virtual cuando personaliza el hardware de la máquina virtual durante el proceso de creación de la máquina virtual o después de la creación de la máquina virtual. Por ejemplo, sería conveniente agregar un disco duro existente que está preconfigurado como disco de arranque.

Durante la creación de la máquina virtual, se agregan un disco duro y una controladora SCSI o SATA a la máquina virtual de forma predeterminada, según el sistema operativo invitado que se seleccione. Si el disco no cumple con sus necesidades, puede eliminarlo y agregar un disco duro existente al final del proceso de creación.

Requisitos previos

- Asegúrese de estar familiarizado con el comportamiento del nodo de dispositivo virtual y la controladora para las diferentes opción de configuración de disco duro virtual.
- Compruebe que posee el privilegio **Máquina virtual.Configuración.Agregar un disco existente** en el almacén de datos o en la carpeta de destino.

Apague la máquina virtual.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Editar configuración** en el menú emergente.

3 En la pestaña **Hardware virtual**, seleccione **Agregar disco duro** y, a continuación, seleccione **Disco duro existente** en el menú desplegable.

4 (opcional) Para eliminar un disco duro existente, desplace el cursor sobre el disco y haga clic en el icono **Quitar** (**X**).

   El disco se quita de la máquina virtual. Si otras máquinas virtuales comparten el disco, los archivos de disco no se eliminan.

5 En la columna Almacén de datos, expanda un almacén de datos, seleccione una carpeta de máquina virtual y seleccione el disco que desea agregar.

   El archivo del disco aparece en la columna Contenido. El menú **Tipo de archivo** muestra los tipos de archivo de compatibilidad para este disco.

6 Haga clic en **Seleccionar** y en **Guardar** para agregar el disco duro existente.

Agregar un disco de memoria persistente en Host Client

Puede agregar un disco duro virtual a una máquina virtual existente, o puede agregar un disco duro cuando personalice el hardware de la máquina virtual durante su proceso de creación. Por ejemplo, es posible que necesite proporcionar espacio de disco adicional para una máquina virtual existente con una gran carga de trabajo. Durante la creación de la máquina virtual, sería conveniente agregar un disco duro que esté configurado previamente como disco de arranque.

Durante la creación de la máquina virtual, se agregan un disco duro y una controladora SCSI o SATA a la máquina virtual de forma predeterminada, según el sistema operativo invitado que se seleccione. Si el disco no cumple con sus necesidades, puede eliminarlo y agregar un disco duro existente al final del proceso de creación.

Requisitos previos

- Compruebe que conoce bien las opciones de configuración y las advertencias para agregar discos duros virtuales. Consulte Configurar un disco virtual.
- Antes de agregar discos de más de 2 TB a una máquina virtual, consulte *Administrar máquinas virtuales de vSphere*.
- Compruebe que posee el privilegio **Máquina virtual.Configuración.Agregar disco nuevo** en el almacén de datos o en la carpeta de destino.

Apague la máquina virtual.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Editar configuración** en el menú emergente.

3 En la pestaña **Hardware virtual**, seleccione **Agregar disco duro** y, a continuación, seleccione **Nuevo disco de memoria persistente** en el menú desplegable.

   El disco duro aparece en la lista de dispositivos de hardware virtual. De forma predeterminada, el disco se almacena en el almacén de datos PMem de host local y no se puede cambiar el almacén de datos.

4 (opcional) Configure los ajustes para el nuevo disco duro y haga clic en **Guardar** para cerrar al asistente.

a Expanda **Nuevo disco duro**.

b Introduzca un valor para el tamaño del disco duro y seleccione las unidades en el menú desplegable.

Nota Todos los discos duros de memoria persistente y los módulos NVDIMM que se agregan a la máquina virtual comparten los mismos recursos PMem. Por lo tanto, debe ajustar el tamaño de los dispositivos de memoria persistente recién agregados conforme a la cantidad de PMem disponible para el host. Si alguna parte de la configuración requiere atención, el asistente se lo avisará.

c En el menú desplegable **Recursos compartidos**, seleccione un valor para la asignación de recursos compartidos al disco virtual.

Recursos compartidos es un valor que representa la medición relativa para controlar el ancho de banda del disco. Los valores Bajo, Normal, Alto y Personalizado se comparan con la suma de todos los recursos compartidos de todas las máquinas virtuales en el host.

d En el menú desplegable **Ubicación de controladora**, seleccione la ubicación de la controladora que utiliza el nuevo disco duro.

e Seleccione un modo del disco.

Opción	Descripción
Dependiente	Se incluyen discos dependientes en las instantáneas.
Independiente-persistente	Los discos en modo persistente se comportan como discos de equipos físicos convencionales. Todos los datos que se escriben en un disco en modo persistente se escriben de forma permanente en el disco.
Independiente-no persistente	Los cambios en los discos en modo no persistente se descartan cuando se apaga o se restablece la máquina virtual. El disco virtual vuelve al mismo estado cada vez que se reinicia la máquina virtual. Los cambios en el disco se escriben y se leen desde un archivo de registro de rehacer que se elimina al apagar o restablecer.

Usar discos compartidos para dar prioridad a máquinas virtuales en el VMware Host Client

Es posible cambiar los recursos de disco de una máquina virtual. Si varias máquinas virtuales acceden al mismo almacén de datos de VMFS y al mismo número de unidad lógica (LUN), use discos compartidos para dar prioridad al nivel de acceso que las máquinas virtuales tienen en los recursos. Los discos compartidos distinguen las máquinas virtuales con prioridad alta de aquellas con prioridad baja.

Puede asignar el ancho de banda de E/S del host a los discos duros virtuales de una máquina virtual. No puede agrupar E/S de disco en un clúster.

El valor de recursos compartidos representa la métrica relativa para el control del ancho de banda de disco que reciben todas las máquinas virtuales.

Los discos compartidos solo son pertinentes dentro de un host determinado. Los recursos compartidos asignados a las máquinas virtuales de un host no afectan a las máquinas virtuales de los demás hosts.

Puede seleccionar una limitación de IOP, la cual establece un límite superior para los recursos de almacenamiento que se asignan a una máquina virtual. El valor de IOPS corresponde a la cantidad de operaciones de E/S por segundo.

Requisitos previos

Apague la máquina virtual.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Editar configuración** en el menú emergente.

3 En la pestaña **Hardware virtual**, expanda el disco duro para ver las opciones del disco.

4 En el menú desplegable **Recursos compartidos**, seleccione un valor para los recursos compartidos que deben asignarse a la máquina virtual.

5 Si seleccionó la opción **Personalizado**, especifique una cantidad de recursos compartidos en el cuadro de texto.

6 En el cuadro de texto **Límite: IOPS**, especifique el límite superior de los recursos de almacenamiento que se deben asignar a la máquina virtual o seleccione la opción **Ilimitado**.

7 Haga clic en **Guardar**.

Configurar la controladora de máquinas virtuales en VMware Host Client

En VMware Host Client, puede agregar varias controladoras a las máquinas virtuales, por ejemplo, controladoras USB, SCSI, Paravirtual SCSI y SATA. También puede cambiar la configuración de uso compartido de bus de SCSI y el tipo de controladora SCSI.

Agregar una controladora USB a una máquina virtual en VMware Host Client

Se pueden agregar controladoras USB a las máquinas virtuales con el fin de admitir el acceso directo a USB en un host ESXi o desde un equipo cliente hacia una máquina virtual.

En vSphere Client, puede agregar una controladora xHCI y una controladora EHCI+UHCI. Desde la versión de hardware 11 hasta la versión de hardware 16, se admiten ocho puertos de hub raíz por controladora xHCI (cuatro puertos lógicos USB 3.1 SuperSpeed y cuatro puertos lógicos USB 2.0). Con la versión 17 del hardware, se admiten ocho puertos de hub raíz por controladora xHCI (cuatro puertos lógicos USB 3.1 SuperSpeedPlus y cuatro puertos lógicos USB 2.0).

Las condiciones para agregar una controladora varían, según la versión del dispositivo, el tipo de acceso directo (equipo cliente o host) y el tipo de sistema operativo invitado.

Tabla 3-3. Compatibilidad con controladoras USB

Tipo de controladora	Versión de dispositivo USB compatible	Compatible para acceso directo desde un host ESXi a una máquina virtual	Compatible para acceso directo desde un equipo cliente a una máquina virtual
EHCI+UHCI	2.0 y 1.1	Sí	Sí
xHCI	3.1, 2.0 y 1.1	Sí Solo para dispositivos USB 3.1, 2.0 y 1.1.	Sí Windows 8 o versiones posteriores, Windows Server 2012 o versiones posteriores, o un sistema operativo invitado de Linux con un kernel 2.6.35 o una versión posterior.

Para los sistemas Mac OS X, la controladora EHCI+UHCI está habilitada de forma predeterminada y es necesaria para el acceso de un teclado y un mouse USB.

Para máquinas virtuales con sistemas operativos invitados Windows o Linux, puede agregar una o dos controladoras de diferentes tipos. No es posible agregar dos controladoras del mismo tipo.

Para el acceso directo mediante USB desde un host ESXi hacia una máquina virtual, el árbitro de USB puede supervisar 15 controladoras USB como máximo. Si el sistema incluye más de 15 controladoras y se conectan dispositivos USB a ellas, los dispositivos no estarán disponibles para la máquina virtual.

Requisitos previos

- Compruebe que los hosts ESXi tengan módulos y hardware de controladoras USB que sean compatibles con dispositivos USB 3.1, 2.0 y 1.1.
- Compruebe que los equipos cliente tengan módulos y hardware de controladoras USB que sean compatibles con dispositivos USB 3.1, 2.0 y 1.1.
- Para usar la controladora xHCI en un sistema operativo Linux invitado, compruebe que el kernel de Linux sea de la versión 2.6.35 o de una versión posterior.
- Compruebe que la máquina virtual esté encendida.
- Privilegio necesario (acceso directo de host ESXi): **Máquina virtual.Configuración.Agregar o eliminar dispositivo**

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Editar configuración** en el menú emergente.

3 En la pestaña **Hardware virtual**, haga clic en **Agregar otro dispositivo** y, a continuación, en **Controladora USB** en el menú desplegable.

   La nueva controladora USB aparece en la parte inferior de la lista de dispositivos Hardware virtual.

4 Amplíe **Nueva controladora USB** para cambiar el tipo de controladora USB.

   Si aparece un error de compatibilidad, soluciónelo antes de agregar la controladora.

5 Haga clic en **Guardar**.

Pasos siguientes

Agregue uno o más dispositivos a la máquina virtual.

Agregar controladoras SCSI en VMware Host Client

Para agregar controladoras SCSI a una máquina virtual existente, agregue discos duros a números de bus de SCSI sin utilizar.

Al agregar un nuevo disco duro a un número de bus de SCSI sin utilizar, se crea una controladora SCSI nueva.

Requisitos previos

Apague la máquina virtual.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Editar configuración** en el menú emergente.

3 En la pestaña **Hardware virtual**, seleccione **Agregar disco duro** y, a continuación, seleccione **Nuevo disco duro** en el menú desplegable.

4 Expanda el disco duro para ver todas las opciones.

5 En la sección **Ubicación de controlador**, seleccione número de bus de SCSI sin utilizar en el menú desplegable.

   Por ejemplo, la controladora SCSI inicial utiliza los números de bus y de dispositivo 0:0 a 0:15. La segunda controladora SCSI utiliza los números de bus y de dispositivo 1:0 a 1:15.

6 Haga clic en **Guardar**.

Resultados

El nuevo disco duro y la nueva controladora SCSI se crean simultáneamente.

Cambiar la configuración de uso compartido de bus de SCSI en VMware Host Client

Puede establecer el tipo de recurso compartido de bus de SCSI para una máquina virtual e indicar si se debe compartir el bus de SCSI. Según el tipo de recurso compartido, las máquinas virtuales pueden acceder al mismo disco virtual simultáneamente en el mismo servidor o en otro servidor.

Es posible cambiar la configuración de la controladora SCSI de una máquina virtual solamente si la máquina virtual está en un host ESXi.

Requisitos previos

Apague la máquina virtual.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Editar configuración** en el menú emergente.

3 En la pestaña **Hardware virtual**, expanda la controladora SCSI que desee editar.

4 Seleccione el tipo de recurso compartido en la lista **Recursos compartidos de bus de SCSI**.

Opción	Descripción
Ninguno	Los discos virtuales no se pueden compartir con otras máquinas virtuales.
Virtual	Los discos virtuales pueden compartirse con las máquinas virtuales en el mismo servidor.
Físico	Los discos virtuales pueden compartirse con las máquinas virtuales en cualquier servidor.

5 Haga clic en **Guardar**.

Cambiar tipo de controladora SCSI en VMware Host Client

Puede asociar discos virtuales y RDM a las máquinas virtuales mediante la configuración de una controladora SCSI virtual en estas.

La elección de controladora SCSI no incide sobre si el disco virtual es un disco de IDE o SCSI. El adaptador IDE siempre es ATAPI. El valor predeterminado para el sistema operativo invitado ya está seleccionado. Los sistemas operativos invitados más antiguos tienen un adaptador BusLogic como controladora predeterminada.

Se crea una máquina virtual LSI Logic y agrega un disco virtual que utiliza adaptadores BusLogic, la máquina virtual arranca desde el disco de adaptadores de BusLogic. LSI Logic SAS está disponible solo para máquinas virtuales con versión de hardware 7 o posteriores. Es posible que los discos con instantáneas no experimenten beneficios en el rendimiento cuando se utilizan en adaptadores LSI Logic SAS, VMware Paravirtual y LSI Logic Parallel.

Precaución Si cambia el tipo de controladora SCSI, se podría producir un error en el arranque de la máquina virtual.

Requisitos previos

Apague la máquina virtual.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.
2 Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Editar configuración** en el menú emergente.
3 Haga clic en la pestaña **Hardware virtual** y expanda una controladora SCSI.
4 Seleccione el tipo de controladora SCSI en el menú desplegable.
5 Haga clic en **Guardar**.

Acerca de las controladoras VMware Paravirtual SCSI

Las controladoras VMware Paravirtual SCSI son controladoras de almacenamiento de alto rendimiento que pueden incrementar la capacidad de proceso y disminuir el uso de CPU. Estas controladoras son más adecuadas para entornos de almacenamiento de alto rendimiento.

Las controladoras VMware Paravirtual SCSI están disponibles para máquinas virtuales con compatibilidad para ESXi 4.x y posterior. Es posible que los discos de dichas controladoras no adquieran un rendimiento óptimo si contienen snapshots o si la memoria del host ESXi está sobrecargada. Este comportamiento no atenúa la mejora de rendimiento general que se obtiene al utilizar controladoras VMware Paravirtual SCSI en comparación con otras opciones de controladora SCSI.

Para conocer la compatibilidad con la plataforma de la controladora VMware Paravirtual SCSI, consulte la *guía de compatibilidad de VMware* en http://www.vmware.com/resources/compatibility.

Agregar una controladora Paravirtual SCSI en VMware Host Client

Es posible agregar una controladora VMware Paravirtual SCSI de almacenamiento de alto rendimiento para brindar mayor capacidad de proceso y menor uso de CPU.

Las controladoras VMware Paravirtual SCSI son más adecuadas para entornos (especialmente entornos SAN) que ejecutan aplicaciones con gran consumo de E/S.

Requisitos previos

- Compruebe que la máquina virtual tenga un sistema operativo invitado con VMware Tools instalado.
- Compruebe que la máquina virtual esté utilizando la versión de hardware 7 o posteriores.
- Familiarícese con las limitaciones de VMware Paravirtual SCSI. Consulte *Administrar máquinas virtuales de vSphere*.
- Para acceder a los dispositivos de disco de arranque asociados con la controladora VMware Paravirtual SCSI, compruebe que la máquina virtual tenga un sistema operativo invitado Windows 2003 o Windows 2008.
- En algunos sistemas operativos, antes de cambiar el tipo de controladora, se debe crear una máquina virtual con una controladora LSI Logic e instalar VMware Tools.

Apague la máquina virtual.

Procedimiento

1. Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.
2. Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Editar configuración** en el menú emergente.
3. En la pestaña **Hardware virtual**, haga clic en **Agregar otro dispositivo** y seleccione **Controladora SCSI** en el menú desplegable.

   Las nuevas controladoras SCSI aparecen en la lista de hardware.
4. Haga clic en **Nueva controladora SCSI** y seleccione **VMware Paravirtual** en el menú desplegable.
5. Haga clic en **Guardar**.

Agregar una controladora SATA a una máquina virtual en VMware Host Client

Si una máquina virtual tiene varios discos duros o dispositivos de CD/DVD-ROM, puede agregar hasta tres controladoras SATA adicionales para asignar los dispositivos. Al asignar los dispositivos a diferentes controladoras, se mejora el rendimiento y se evita la congestión del tráfico de datos. También se pueden agregar controladoras si necesita superar el límite de treinta dispositivos para una sola controladora.

Es posible arrancar máquinas virtuales desde controladoras SATA y utilizarlas para discos duros virtuales de gran capacidad.

No todos los sistemas operativos invitados son compatibles con las controladoras SATA AHCI. Por lo general, cuando se crean máquinas virtuales con compatibilidad con ESXi 5.5 y versiones posteriores y sistemas operativos invitados Mac OS X, se agrega de forma predeterminada una controladora SATA para el disco duro virtual y los dispositivos de CD/DVD-ROM. La mayoría

de los sistemas operativos invitados, incluido Windows Vista y versiones posteriores, tienen una controladora SATA predeterminada para los dispositivos de CD/DVD-ROM. Para realizar una verificación, consulte la *Guía de compatibilidad de VMware* correspondiente en http://www.vmware.com/resources/compatibility.

Requisitos previos

- Compruebe que la máquina virtual sea compatible con ESXi 5.5 y versiones posteriores.
- Asegúrese de que conoce el comportamiento y las limitaciones de la controladora de almacenamiento. Consulte *Administrar máquinas virtuales de vSphere*.
- Verifique que posea el privilegio **Máquina virtual.Configuración.Agregar o quitar dispositivo** en la máquina virtual.
- Apague la máquina virtual.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Editar configuración** en el menú emergente.

3 En la pestaña **Hardware virtual**, seleccione **Agregar otro dispositivo** y, a continuación, seleccione **Controladora SATA** en el menú desplegable.

   La controladora SATA aparece en la lista de hardware.

4 Haga clic en **Guardar**.

Agregar una controladora de NVMe en VMware Host Client

Si una máquina virtual contiene varios discos duros, es posible agregar hasta cuatro controladoras virtuales NVMe a las que se puedan asignar los discos. Una controladora NVMe reduce significativamente la sobrecarga de software para el procesamiento de la E/S del sistema operativo invitado, en comparación con las controladoras AHCI SATA o SCSI.

Las controladoras NVMe trabajan mejor con los discos virtuales en una matriz de discos basados íntegramente en flash, SSD NVMe local y el almacenamiento de PMem.

Requisitos previos

- Compruebe que la máquina virtual contenga un sistema operativo invitado compatible con NVMe.
- Compruebe que la máquina virtual sea compatible con ESXi 6.5 o posterior.
- Asegúrese de que conoce el comportamiento y las limitaciones de los controladores de almacenamiento. Para obtener más información, consulte la guía *Administración de máquinas virtuales*.
- Compruebe si cuenta con el privilegio **Máquina virtual.Configuración.Agregar disco nuevo** en la máquina virtual.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Editar configuración** en el menú emergente.

3 En la pestaña **Hardware virtual**, haga clic en el icono **Agregar otro dispositivo** y seleccione **Controladora de NVMe** en el menú desplegable.

Resultados

Se agregará una nueva controladora de NVMe a la máquina virtual.

Pasos siguientes

Puede agregar un disco duro a la máquina virtual y asignarla a la controladora NVMe.

Otra configuración de dispositivos de máquinas virtuales en VMware Host Client

Además de configurar los recursos de CPU y memoria de las máquinas virtuales y agregar discos duros y adaptadores de red virtuales, también puede agregar y configurar hardware virtual, como unidades de DVD/CD-ROM, unidades de disquete y dispositivos SCSI. También puede agregar un dispositivo de temporizador de Watchdog virtual (Virtual Watchdog Timer, VWDT), un dispositivo de reloj de precisión y dispositivos PCI.

Agregar una unidad de CD o DVD a una máquina virtual en VMware Host Client

Para agregar una unidad de CD/DVD a una máquina virtual, puede usar una unidad física en un cliente o host, o bien puede usar una imagen ISO.

Si desea agregar una unidad de CD/DVD que cuente con una copia de seguridad en una unidad de USB CD/DVD en el host, debe agregar la unidad como dispositivo SCSI. No se admite la funcionalidad para agregar o quitar dispositivos SCSI en caliente de un host ESXi.

Requisitos previos

Apague la máquina virtual.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Editar configuración** en el menú emergente.

3 En la pestaña **Hardware virtual**, seleccione **Agregar otro dispositivo** y, a continuación, seleccione **Unidad de CD/DVD** en el menú desplegable.

4 Expanda **Unidad de CD/DVD** y seleccione una opción.

Opción	Descripción
Usar unidad física	a Seleccione **Dispositivo del cliente** como la ubicación. b En el menú desplegable **Modo de dispositivo**, seleccione **Emulación de CD-ROM** o **CD-ROM de acceso directo**.
Usar imagen ISO	a Seleccione **Archivo ISO del almacén de datos** como la ubicación. b Introduzca la ruta de acceso y el nombre del archivo de imagen, o bien haga clic en **Examinar** para desplazarse hasta el archivo.

5 Si no desea que la unidad de CD-ROM se conecte cuando se inicie la máquina virtual, desactive la casilla **Conectar al encender**.

6 Seleccione el nodo del dispositivo virtual que utiliza la unidad en la máquina virtual.

7 Haga clic en **Guardar**.

Agregar una unidad de disquete a una máquina virtual en VMware Host Client

Use una unidad física de disquete o una imagen de disquete para agregar una unidad de disquete a una máquina virtual.

ESXi no admite unidades de disquete que están respaldadas por una unidad física de disco flexible en el host.

Requisitos previos

- Apague la máquina virtual.
- Verifique que posea el privilegio **Máquina virtual.Configuración.Agregar o quitar dispositivo** en la máquina virtual.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Editar configuración** en el menú emergente.

3 En la pestaña **Hardware virtual**, seleccione **Agregar otro dispositivo** y, a continuación, seleccione **Unidad de disquete** en el menú desplegable.

   La unidad de disquete aparece en la lista de hardware.

4 Expanda **Unidad de disquete** y seleccione el tipo de dispositivo que desea usar.

Opción	Descripción
Dispositivo cliente	Seleccione esta opción para conectar el dispositivo de disquete a un dispositivo de disquete físico o a una imagen de disquete `.flp` en el sistema desde el que accede a VMware Host Client .
Usar imagen de disquete existente	a Seleccione esta opción para conectar el dispositivo virtual a una imagen de disquete existente en un almacén de datos accesible para el host. b Haga clic en **Examinar** y seleccione la imagen de disquete.

5 (opcional) Seleccione **Conectar al encender** para configurar el dispositivo cuando se encienda la máquina virtual.

6 Haga clic en **Guardar**.

Agregar un dispositivo USB a una máquina virtual en VMware Host Client

Al utilizar VMware Host Client, puede agregar un dispositivo USB a una máquina virtual.

Requisitos previos

- Compruebe que haya una controladora USB. Consulte Agregar una controladora USB a una máquina virtual en VMware Host Client.
- Agregue un dispositivo USB físico al host ESXi donde está ubicada la máquina virtual enchufándolo en el host.

Nota Si el host ESXi no tiene dispositivos USB disponibles, no podrá agregar un dispositivo USB a la máquina virtual.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Editar configuración** en el menú emergente.

3 En la pestaña **Hardware virtual**, seleccione **Agregar otro dispositivo** y, a continuación, seleccione **Dispositivo USB** en el menú desplegable.

El dispositivo USB aparece en la lista de hardware de dispositivos de hardware disponibles para la máquina virtual.

4 En el menú desplegable **Dispositivo USB**, seleccione el dispositivo USB que desea agregar a la máquina virtual.

5 Haga clic en **Guardar**.

Agregar un controlador de sonido a una máquina virtual en VMware Host Client

Al utilizar VMware Host Client, puede agregar un controlador de sonido a una máquina virtual.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Editar configuración** en el menú emergente.

3 En la pestaña **Hardware virtual**, seleccione **Agregar otro dispositivo** y, a continuación, seleccione **Controlador de sonido** en el menú desplegable.

   El controlador de sonido aparece en la lista de dispositivos de hardware disponibles para la máquina virtual.

4 En el menú desplegable **Tarjeta de sonido**, seleccione el controlador de sonido que desea conectar a la máquina virtual.

5 Haga clic en **Guardar**.

Configurar puertos serie y paralelos en VMware Host Client

Los puertos serie y paralelos son interfaces para la conexión de periféricos con la máquina virtual. El puerto serie virtual puede conectarse a un puerto serie físico o a un archivo en el equipo host. También puede usarse para establecer una conexión directa entre dos máquinas virtuales o una conexión entre una máquina virtual y una aplicación en el equipo host. Puede agregar puertos serie o paralelos y cambiar la configuración del puerto serie.

Agregar un puerto serie a una máquina virtual en VMware Host Client

Una máquina virtual puede utilizar hasta cuatro puertos serie virtuales. Puede conectar el puerto serie virtual a un puerto serie físico o a un archivo en el equipo host. También puede utilizar una canalización designada en el lado del host para configurar una conexión directa entre dos máquinas virtuales o una conexión entre una máquina virtual y una aplicación en el equipo host. Además, puede utilizar un puerto o un URI de concentrador de puertos serie virtuales (vSPC) para conectar un puerto serie por medio de la red.

Requisitos previos

- Familiarícese con los diferentes tipos de soportes físicos a los que puede acceder el puerto, las conexiones vSPC y cualquier condición que pueda aplicarse. Consulte *Administrar máquinas virtuales de vSphere*.
- Para conectar un puerto serie a la red, agregue un conjunto de reglas de firewall. Consulte *Administrar máquinas virtuales de vSphere*.
- Privilegio necesario: **Máquina virtual.Configuración.Agregar o quitar dispositivo**

  Apague la máquina virtual.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Editar configuración** en el menú emergente.

3 En la pestaña **Hardware virtual**, seleccione **Agregar otro dispositivo** y, a continuación, seleccione **Puerto serie**.

El puerto serie aparece en la lista de hardware.

4 En la lista de hardware, expanda el puerto serie y seleccione el tipo de puerto de medios para acceder.

Opción	Descripción
Usar archivo de salida	Desplácese hasta la ubicación del archivo en el host para almacenar el resultado del puerto serie virtual.
Usar puerto serie físico	Seleccione el puerto en el menú desplegable.
Usar conexión indicada	a Escriba un nombre para la conexión en el campo **Nombre de la conexión**. b Seleccione **Extremo cercano** y **Extremo lejano** de la canalización en los menús desplegables.
Utilizar red	a En el menú desplegable, **Dirección** seleccione **Servidor** o **Cliente**. b Escriba el URI del puerto. El URI es el extremo remoto del puerto serie al cual se debe conectar el puerto serie de la máquina virtual. c Si se usa vSPC como paso intermedio para acceder a todas las máquinas virtuales a través de una sola dirección IP, seleccione **Usar concentrador de puerto serie virtual** e introduzca la ubicación URI de vSPC.

5 (opcional) Anule la selección de **Conectar al encenderse** si no desea que el dispositivo con puerto paralelo se conecte cuando se encienda la máquina virtual.

6 Haga clic en **Guardar**.

Ejemplo: Establecer conexiones de red de puerto serie con un cliente o servidor sin parámetros de autenticación

Si no se usa vSPC y se configura la máquina virtual con un puerto serie conectado como servidor con un URI `telnet://:12345`, es posible conectarse al puerto serie de la máquina virtual desde el sistema operativo Linux o Windows.

```
telnet yourESXiServerIPAddress 12345
```

De forma similar, si se ejecuta el servidor de Telnet en el sistema Linux en el puerto 23 (`telnet://yourLinuxBox:23`), configure la máquina virtual como un URI de cliente.

```
telnet://yourLinuxBox:23
```

La máquina virtual inicia la conexión con el sistema Linux en el puerto 23.

Agregar un puerto paralelo en una máquina virtual en VMware Host Client

Para conectar dispositivos periféricos a máquinas virtuales, como impresoras y escáneres, se puede usar un puerto paralelo. La salida de dichos dispositivos se envía a un archivo en el equipo host.

Nota Para agregar un puerto paralelo a una máquina virtual que se ejecuta en un host ESXi 4.1 o anterior, también puede seleccionar enviar la salida a un puerto paralelo físico en el host. Esta opción no está disponible con hosts ESXi 5.0 y versiones posteriores.

Requisitos previos

- Apague la máquina virtual.
- Verifique que posea el privilegio **Máquina virtual.Configuración.Agregar o quitar dispositivo** en la máquina virtual.

Procedimiento

1. Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.
2. Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Editar configuración** en el menú emergente.
3. En la pestaña **Hardware virtual**, seleccione **Agregar otro dispositivo** y, a continuación, seleccione **Puerto paralelo**.

   El puerto paralelo aparece en la lista de hardware.
4. Expanda el puerto paralelo y en el campo Conexión, vaya a la carpeta en la que desee crear el archivo.

   La ruta del archivo aparece en el cuadro de texto **Conexión**.
5. (opcional) Seleccione **Conectar al encender** para configurar el dispositivo cuando se encienda la máquina virtual.
6. Haga clic en **Guardar**.

Usar un temporizador de Watchdog virtual

Para garantizar la independencia relacionada con el rendimiento del sistema dentro de una máquina virtual, puede agregar un dispositivo de temporizador de Watchdog virtual (Virtual Watchdog Timer, VWDT). Si el sistema operativo invitado deja de responder y no puede recuperarse por su cuenta debido a problemas o errores de software, el VWDT espera un período de tiempo predefinido y, a continuación, reinicia el sistema.

Puede habilitar el VWDT para que se inicie mediante el sistema operativo invitado o el firmware de EFI o BIOS. Si seleccionó el VWDT para que se inicie mediante el firmware de EFI o BIOS, este se iniciará antes de que arranque la sistema operativo invitado.

El VWDT tiene una función importante en las soluciones de agrupación en clústeres basadas en invitado, donde cada máquina virtual del clúster puede recuperarse por cuenta propia si se produce un error.

Agregar un dispositivo temporizador de Watchdog virtual a una máquina virtual en la instancia de VMware Host Client

Puede agregar un dispositivo temporizador de Watchdog virtual a una máquina virtual para impedir que en ella se produzca un error de sistema operativo invitado durante un período de tiempo prolongado.

Requisitos previos

- Apague la máquina virtual.
- Compruebe que posee el privilegio **Máquina virtual.Configuración.Agregar o eliminar dispositivo** en la máquina virtual.
- Compruebe que el sistema operativo invitado de la máquina virtual sea compatible con el dispositivo VWDT.
- Compruebe que la versión de hardware virtual sea 17.

Procedimiento

1. Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.
2. Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Editar configuración** en el menú emergente.
3. En la pestaña **Hardware virtual**, seleccione **Agregar otro dispositivo** y haga clic en **Temporizador de Watchdog**.

   El dispositivo temporizador de Watchdog aparece en la lista de hardware.
4. (opcional) Seleccione **Iniciar con arranque BIOS/EFI** para iniciar el temporizador de Watchdog mediante el firmware de BIOS o EFI.

   Al seleccionar esta opción, el dispositivo VWDT se inicia antes del sistema operativo invitado. Si el arranque del sistema operativo invitado tarda demasiado tiempo o no admite el temporizador de Watchdog, es posible que el dispositivo reinicie constantemente la máquina virtual.
5. Haga clic en **Guardar**.

Agregar un dispositivo de reloj de precisión a una máquina virtual en VMware Host Client

Un reloj de precisión es un dispositivo virtual que se ejecuta en una máquina virtual y que accede a la hora del sistema de un host. Al agregar un reloj de precisión a una máquina virtual, se garantiza que la hora está sincronizada y que las marcas de tiempo tengan una gran precisión.

Requisitos previos

- Apague la máquina virtual.
- Compruebe que la versión de hardware virtual sea 17.

- Compruebe que posee el privilegio **Máquina virtual.Configuración.Agregar o eliminar dispositivo** en la máquina virtual.
- Compruebe que posee el privilegio **Máquina virtual.Configuración.Modificar configuración de dispositivos** en la máquina virtual.

Procedimiento

1 En el inventario de VMware Host Client, haga clic en **Máquinas virtuales**.

2 Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Editar configuración** en el menú emergente.

3 En la pestaña **Hardware virtual**, haga clic en **Agregar otro dispositivo** y seleccione **Reloj de precisión**.

   El dispositivo de reloj de precisión aparece en la lista de hardware.

4 (opcional) Seleccione el protocolo de sincronización de hora.

5 Haga clic en **Guardar**.

Agregar un dispositivo PCI a una máquina virtual en VMware Host Client

DirectPath I/O permite que el sistema operativo invitado de una máquina virtual acceda directamente a los dispositivos PCI y PCIe físicos conectados a un host. Con esta tecnología, puede conectar cada máquina virtual a un máximo de dieciséis dispositivos PCI físicos. Puede usar Dynamic DirectPath I/O para asignar varios dispositivos de acceso directo PCI a una máquina virtual. A partir de vSphere 7.0, puede identificar los dispositivos de acceso directo PCI por su proveedor y nombre de modelo.

Nota Algunas operaciones de máquina virtual dejan de estar disponibles cuando se agrega un dispositivo de acceso directo PCI o PCIe a la máquina virtual.

Para obtener información sobre la configuración de la etiqueta de hardware, consulte Cambiar la etiqueta de hardware en VMware Host Client.

Requisitos previos

- Apague la máquina virtual.
- Compruebe que posee el privilegio **Máquina virtual.Configuración.Agregar o eliminar dispositivo** en la máquina virtual.
- Compruebe que los dispositivos PCI estén conectados al host y marcados como disponibles para acceso directo.
- Si desea agregar un dispositivo PCI dinámico a una máquina virtual, compruebe que la versión de hardware virtual sea la 17.

Procedimiento

1 En el inventario de VMware Host Client, haga clic en **Máquinas virtuales**.

2 Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Editar configuración** en el menú emergente.

3 En la pestaña **Hardware virtual**, haga clic en **Agregar otro dispositivo** y seleccione un dispositivo.

Opción	Acción
Dispositivo PCI	a Haga clic en **Dispositivo PCI**. Un nuevo dispositivo aparece en la lista de hardware. b En el menú desplegable, seleccione un dispositivo PCI para conectar a la máquina virtual.
Dispositivo PCI dinámico	a Haga clic en **Dispositivo PCI dinámico**. Un nuevo dispositivo aparece en la lista de hardware. b Expanda **Nuevo dispositivo PCI** y, en el menú desplegable, seleccione los dispositivos de acceso directo PCI que desea conectar a la máquina virtual. Puede identificar los dispositivos de acceso directo PCI por proveedor, nombre de modelo y etiqueta de hardware. Las etiquetas de hardware, si están presentes, se muestran entre paréntesis. **Nota** Cuando se agrega un dispositivo PCI a una máquina virtual, el tamaño de memoria total de la máquina virtual se reserva automáticamente.

4 Haga clic en **Guardar**.

Proteger máquinas virtuales con Intel Software Guard Extensions

Al utilizar vSphere Client, puede configurar Virtual Software Guard Extensions (vSGX) de Intel® para las máquinas virtuales y proporcionar seguridad adicional a las cargas de trabajo.

Algunas CPU modernas de Intel implementan una extensión de seguridad llamada Intel® Software Guard Extensions (Intel SGX). Intel SGX es una tecnología específica de procesador que define regiones privadas de memoria denominadas enclaves. Intel SGX protege el contenido de los enclaves contra divulgación y modificación de manera tal que el código que se ejecuta fuera de los enclaves no pueda acceder a ellos.

vSGX permite que las máquinas virtuales utilicen la tecnología Intel SGX si está disponibles en el hardware. Para usar vSGX, el host ESXi debe estar instalado en una CPU compatible con SGX, y SGX debe estar habilitado en el BIOS del host ESXi. Puede utilizar vSphere Client para habilitar SGX para una máquina virtual.

Habilitar vSGX en una máquina virtual de VMware Host Client

Para evitar que el contenido de los enclaves se divulgue o se modifique, puede habilitar vSGX en una máquina virtual en VMware Host Client.

Algunas operaciones y características no son compatibles con SGX.

- Migrar con Storage vMotion

- Suspender o reanudar la máquina virtual
- Crear una instantánea de la máquina virtual
- Fault Tolerance
- Habilitar la integridad del invitado (GI, base de la plataforma para VMware AppDefense 1.0)

Requisitos previos

- Apague la máquina virtual.
- Compruebe que la máquina virtual utilice firmware EFI.
- Compruebe que la versión del host ESXi sea 7.0 o posterior.
- Compruebe que el sistema operativo invitado de la máquina virtual sea Linux, Windows 10 (64 bits) o posterior, o Windows Server 2016 (64 bits) o posterior.
- Compruebe que posee el privilegio **Máquina virtual.Configuración.Modificar configuración de dispositivos** en la máquina virtual.
- Compruebe que el host ESXi esté instalado en una CPU compatible con SGX y que SGX esté habilitado en el BIOS del host ESXi. Para obtener información sobre las CPU admitidas, consulte https://kb.vmware.com/s/article/71367.

Procedimiento

1. En el inventario de VMware Host Client, haga clic en **Máquinas virtuales**.
2. Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Editar configuración** en el menú emergente.
3. En la pestaña **Hardware virtual**, expanda **Dispositivos de seguridad**.
4. Active la casilla **Habilitar**.
5. En **Tamaño de memoria caché de página de enclave**, introduzca un nuevo valor en el cuadro de texto y seleccione el tamaño en MB o GB en el menú desplegable.

   Nota El tamaño de la memoria caché de la página de enclave debe ser un múltiplo de 2.

6. En el menú desplegable **Configuración de control de inicio**, seleccione el modo adecuado.

Opción	Acción
Bloqueado	Habilita la configuración del enclave de inicio. En **Hash de clave pública de enclave de inicio**, introduzca un hash SHA256 válido. La clave de hash SHA256 debe contener 64 caracteres.
Desbloqueado	Habilita la configuración del enclave de inicio del sistema operativo invitado.

7. Haga clic en **Guardar**.

Deshabilitar vSGX en una máquina virtual de VMware Host Client

Para deshabilitar vSGX en una máquina virtual, puede utilizar VMware Host Client.

Procedimiento

1 En el inventario de VMware Host Client, haga clic en **Máquinas virtuales**.
2 Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Editar configuración** en el menú emergente.
3 En la pestaña **Hardware virtual**, expanda **Dispositivos de seguridad**.
4 Desactive la casilla **Habilitar** y haga clic en **Guardar**.

Resultados

vSGX se deshabilita en la máquina virtual.

Administrar máquinas virtuales en VMware Host Client

Después de crear una máquina virtual en VMware Host Client, puede realizar diferentes tareas en la máquina virtual, entre ellas, eliminar la máquina virtual del host, quitar la máquina virtual de un almacén de datos, volver a registrar la máquina virtual en un almacén de datos, etc. Puede también devolver la máquina virtual al host.

Acceder a una máquina virtual en VMware Host Client

Puede acceder a las máquinas virtuales del host en el que ha iniciado sesión para configurar el hardware y las opciones de las máquinas virtuales, realizar tareas administrativas y realizar tareas básicas de solución de problemas.

Para mostrar una máquina virtual en el inventario de VMware Host Client, encienda la máquina virtual.

Procedimiento

- ◆ Para acceder a las máquinas virtuales que están disponibles en el host en el que inició sesión, haga clic en **Máquinas virtuales** desde el inventario de VMware Host Client.

Resultados

La lista de máquinas virtuales disponibles se muestra en **Máquinas virtuales**.

Ahora puede editar la configuración de las máquinas virtuales y realizar diferentes tareas administrativas y de solución de problemas en las máquinas virtuales de la lista.

Estados de energía de una máquina virtual en la VMware Host Client

Las operaciones de alimentación básicas de una máquina virtual incluyen encender, apagar, suspender y restablecer.

Para obtener información sobre cómo cambiar los estados de energía de las máquinas virtuales, consulte Configurar los estados de energía de máquinas virtuales en VMware Host Client.

Requisitos previos

- Compruebe que posee los privilegios **Máquina virtual.Interacción.Encendido**.
- Compruebe que posee los privilegios **Máquina virtual.Interacción.Apagado**.
- Compruebe que posee los privilegios **Máquina virtual.Interacción.Suspender**.
- Compruebe que posee los privilegios **Máquina virtual.Interacción.Restablecer**.

Procedimiento

1 En el inventario de VMware Host Client, haga clic en **Máquinas virtuales**.

2 Haga clic con el botón derecho en una máquina virtual y seleccione una operación de energía.

Opción	Descripción
Encender ( )	Enciende una máquina virtual cuando se detiene la máquina virtual.
Apagar ( )	Apaga una máquina virtual y apaga el sistema operativo invitado. El apagado de una máquina virtual puede provocar la pérdida de datos.
Suspender ()	Suspende la máquina virtual en ejecución y la deja conectada a la red. Cuando reanuda una máquina virtual suspendida, la máquina virtual sigue funcionando en el mismo punto en el que estaba cuando se suspendió.
Restablecer ()	Apaga y reinicia el sistema operativo invitado sin apagar la máquina virtual.

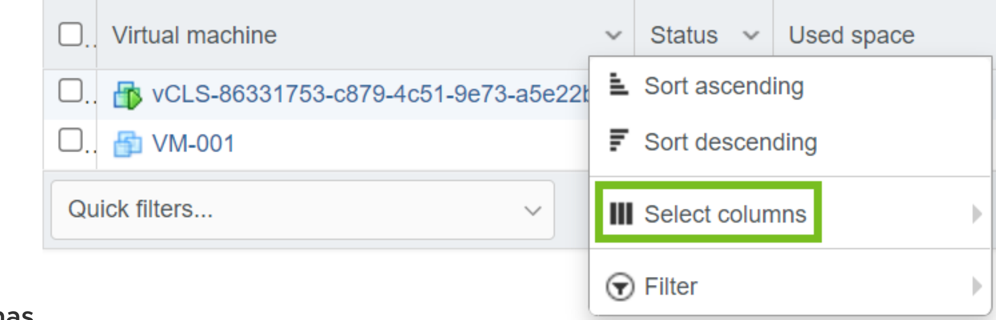
Usar configuración de columnas de máquinas virtuales en VMware Host Client

El panel de máquinas virtuales de VMware Host Client permite configurar la información que desea que aparezca. Se pueden mostrar u ocultar diferentes columnas, como el estado, el espacio utilizado, el nombre del host, la CPU del host, etc.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 En la lista de máquinas virtuales, haga clic en el icono de flecha hacia abajo que aparece junto al título de cualquier columna y seleccione **Seleccionar columnas**.



Aparecerá entonces la lista con todas las columnas disponibles.

3 Seleccione la información que desee que se vea en el panel de máquinas virtuales.

Quitar máquinas virtuales de un host en VMware Host Client

Puede cancelar el registro una máquina virtual si quiere mantenerla en el almacén de datos, pero ya no se mostrará en el inventario de VMware Host Client.

Requisitos previos

Apague la máquina virtual.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Cancelar el registro**.

3 Para confirmar que desea quitar la máquina virtual del inventario, haga clic en **Sí**.

Resultados

El host elimina la máquina virtual del inventario y no realiza ningún seguimiento más de su condición.

Quitar máquinas virtuales de un almacén de datos en VMware Host Client

Si necesita liberar espacio en el almacén de datos, puede eliminar las máquinas virtuales que ya no necesite. Al quitar una máquina virtual del inventario de VMware Host Client, se eliminan del almacén de datos todos los archivos de la máquina virtual, incluidos los archivos de configuración y de discos virtuales. Puede eliminar varias máquinas virtuales.

Requisitos previos

- Apague la máquina virtual.

- Compruebe que la máquina virtual no comparta el disco con otra máquina virtual. Si dos máquinas virtuales comparten un disco, no se eliminan los archivos de disco.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Seleccione una o varias de las casillas de verificación que aparecen junto a las máquinas virtuales que desea eliminar y, a continuación, seleccione **Acciones > Eliminar**.

   Se abrirá el cuadro de diálogo **Eliminar máquinas virtuales**.

3 Haga clic en **Eliminar**.

Registrar una máquina virtual en VMware Host Client

Si se quita una máquina virtual o una plantilla de un host, pero no se las quita del almacén de datos del host, se las puede devolver al inventario del host.

Procedimiento

1 Haga clic en **Almacenamiento** en el inventario de VMware Host Client.

2 Haga clic con el botón derecho en un almacén de datos de la lista y, a continuación, en **Registrar una máquina virtual**.

3 Seleccione la máquina virtual que desee registrar de la lista y haga clic en **Registrar**.

Usar instantáneas para administrar máquinas virtuales

Las snapshots conservan el estado y los datos de una máquina virtual en el momento que crea dicha snapshot. Cuando se crea una instantánea de una máquina virtual, la máquina virtual no se ve afectada y solamente se copia y se almacena una imagen de esta en un estado determinado. Las snapshots son útiles cuando es necesario volver en repetidas ocasiones al mismo estado de la máquina virtual, pero no se desea crear varias máquinas virtuales.

Debe crea varias snapshots de una máquina virtual para crear posiciones de restauración en un proceso lineal. Con varias instantáneas, puede guardar muchas posiciones para poder realizar diversos tipos de procesos de trabajo. Las snapshots funcionan en máquinas virtuales individuales. Para crear snapshots de varias máquinas virtuales, por ejemplo, snapshots de todos los miembros de un equipo, es necesario que cree una snapshot separada de la máquina virtual de cada miembro del equipo.

Las instantáneas son útiles como una solución a corto plazo para probar software con efectos desconocidos o potencialmente dañinos. Por ejemplo, puede utilizar una snapshot como punto de restauración durante un proceso lineal o iterativo, como la instalación de paquetes de actualización o durante un proceso de ramificación, como la instalación de diferentes versiones de un programa. Con el uso de snapshots se garantiza que cada instalación comience desde una línea base idéntica.

Con las instantáneas, es posible conservar una línea base antes de realizar cambios en una máquina virtual en un árbol de instantáneas.

Hay varias operaciones disponibles en el Administrador de instantáneas de VMware Host Client para crear y administrar instantáneas de máquinas virtuales y árboles de instantáneas. Estas operaciones permiten crear instantáneas, restaurar cualquier instantánea en la jerarquía de instantáneas, eliminar instantáneas, etc. Puede crear extensos árboles de instantáneas que puede usar para guardar el estado de una máquina virtual en un momento específico y restaurar posteriormente el estado de la máquina virtual. Cada rama en un árbol de snapshots puede tener hasta 32 snapshots.

Una snapshot conserva la siguiente información:

- La configuración de la máquina virtual. El directorio de la máquina virtual, que incluye los discos que se agregaron o se modificaron después de que se tomó la instantánea.
- El estado de energía. La máquina virtual puede encenderse, apagarse o suspenderse.
- El estado del disco. El estado de todos los discos virtuales de la máquina virtual.
- (Opcional) El estado de la memoria. El contenido de la memoria de la máquina virtual.

Jerarquía de snapshots

El Administrador de snapshots presenta una jerarquía de snapshots como un árbol con una o más ramas. Las instantáneas de la jerarquía tienen relaciones primarias y secundarias. En los procesos lineales, cada instantánea tiene una instantánea primaria y una secundaria, excepto la última instantánea, que no tiene instantáneas secundarias. Cada snapshot primaria puede tener una o más secundarias. Puede volver a la snapshot primaria actual o restaurar cualquier snapshot primaria o secundaria en el árbol y crear más snapshots desde ella. Cada vez que restaure una snapshot y cree otra, se crea una rama o snapshot secundaria.

Snapshots primarias

La snapshot de la primera máquina virtual que cree es la snapshot primaria de base. La snapshot primaria es la versión guardada más reciente del estado actual de la máquina virtual. Al tomar una snapshot se crea un archivo de disco delta para cada disco conectado a la máquina virtual y, opcionalmente, un archivo de memoria. Los archivos de disco delta y el archivo de memoria se almacenan con el archivo `.vmdk`. La snapshot primaria siempre es aquella que aparece inmediatamente sobre el icono Usted está aquí en el Administrador de snapshots. Si se revierte a una snapshot o se restaura una, esa snapshot se convierte en la primaria del estado actual de Usted está aquí.

Nota La snapshot primaria no siempre es la que se sacó más recientemente.

Snapshots secundarias

Una instantánea de una máquina virtual tomada después de la instantánea primaria. Cada instantánea secundaria contiene archivos diferenciales para cada disco virtual conectado y, opcionalmente, un archivo de memoria que apunta desde el estado actual del disco virtual (Usted está aquí). Los archivos diferenciales de cada snapshot secundaria se fusionan con cada snapshot secundaria anterior hasta que se llega a los discos primarios. Un disco secundario puede convertirse después en un disco primario para futuros discos secundarios.

La relación entre snapshots primarias y secundarias puede cambiar si tiene varias ramas en el árbol de snapshots. Una snapshot primaria puede tener más de una snapshot secundaria. Muchas snapshots no tienen snapshots secundarias.

Importante No maneje de forma manual discos secundarios individuales o cualquier archivo de configuración de snapshots, ya que si lo hace, se puede ver perjudicado el árbol de snapshots y ocasionar una pérdida de datos. Esta restricción incluye el cambio de tamaño del disco y las modificaciones al disco base primario mediante `vmkfstools`.

Comportamiento de las snapshots

Al tomar una snapshot se conserva el estado del disco en un momento específico gracias a la creación de una serie de discos delta para cada disco virtual conectado o RDM virtual y, opcionalmente, se conserva el estado de la memoria y la energía mediante la creación de un archivo de memoria. Cuando se toma una snapshot se crea un objeto de snapshot en el Administrador de snapshots que representa el estado y la configuración de la máquina virtual.

Cada instantánea crea un archivo de disco delta `.vmdk` adicional. En el momento en que se crea una snapshot, el mecanismo de snapshot impide que el sistema operativo invitado escriba en el archivo `.vmdk` base y, en su lugar, dirige todas las escrituras al archivo de disco delta. El disco delta representa la diferencia entre el estado actual del disco virtual y el estado en el momento en que se tomó la snapshot anterior. Si existe más de una snapshot, los discos delta pueden representar la diferencia entre cada snapshot. Si el sistema operativo invitado escribe en cada bloque del disco virtual, los discos delta pueden expandirse rápidamente y quedar con el mismo tamaño que el disco virtual completo.

Archivos de instantáneas

Al crear una instantánea, captura el estado de la configuración de la máquina virtual y del disco virtual. Si crea una instantánea de memoria, también captura el estado de la memoria de la máquina virtual. Estos estados se guardan en archivos que residen junto con los archivos de base de la máquina virtual.

Archivos de instantáneas

Una instantánea está compuesta por archivos que se almacenan en un dispositivo de almacenamiento compatible. Con la operación Crear instantánea, se crean archivos `.vmdk`, `-delta.vmdk`, `.vmsd` y `.vmsn` . De forma predeterminada, el primer disco delta y todos los discos delta se almacenan en el archivo de base `.vmdk`. Los archivos `.vmsd` y `.vmsn` se almacenan en el directorio de la máquina virtual.

Archivos de discos delta

Un archivo `.vmdk` en el que puede escribir datos el sistema operativo invitado. El disco delta representa la diferencia entre el estado actual del disco virtual y el estado que tenía en el momento en que se creó la instantánea anterior. Cuando se crea una instantánea, se conserva el estado del disco virtual, el sistema operativo invitado deja de escribir datos en él y se crea un disco delta o secundario.

Un disco delta tiene dos archivos. Uno es un pequeño archivo de descriptor que contiene información sobre el disco virtual, como información sobre la geometría y la relación entre elementos primarios y secundarios. El otro es un archivo correspondiente que contiene los datos sin procesar.

Los archivos que conforman el disco delta se denominan discos secundarios o registros de reconstrucción.

Archivo plano

Un archivo `-flat.vmdk` que es uno de dos archivos que conforma el disco base. El disco plano contiene los datos sin procesar del disco base. El archivo no aparece como un archivo independiente en el navegador del almacén de datos.

Archivo de base de datos

Un archivo `.vmsd` que contiene la información de instantáneas de la máquina virtual y el origen de información principal de Administrador de instantáneas. Este archivo contiene entradas de líneas, que definen las relaciones entre las instantáneas y entre los discos secundarios de cada instantánea.

Archivo de memoria

Un archivo `.vmsn` que incluye el estado activo de la máquina virtual. La captura del estado de la memoria de la máquina virtual permite realizar una reversión a un estado de máquina virtual encendida. Con las instantáneas que se crean sin memoria, solo es posible realizar una reversión a un estado de máquina virtual apagada. Las instantáneas creadas con memoria tardan más en generarse que las instantáneas que se crean sin memoria. El tiempo que tarda el host ESXi en escribir la memoria en el disco depende de la cantidad de memoria que la máquina virtual está configurada para usar.

Una operación **Crear instantánea** genera archivos `.vmdk`, `-delta.vmdk`, `vmsd` y `vmsn`.

Archivo.	Descripción
vmname-*número*.vmdk y *vmname*-*número*-delta.vmdk	Archivo de instantánea que representa la diferencia entre el estado actual del disco virtual y el estado que tenía en el momento en que se creó la instantánea anterior. El nombre de archivo usa la sintaxis `S1vm-000001.vmdk`, donde `S1vm` corresponde al nombre de la máquina virtual y el número de seis dígitos (`000001`) se basa en los archivos que ya existen en el directorio. El número no tiene en cuenta la cantidad de discos que están conectados a la máquina virtual.
vmname.vmsd	La base de datos de la información de instantáneas de la máquina virtual y el origen de información principal de Administrador de instantáneas.
vmname.Instantánea*número*.vmsn	El estado en la memoria de la máquina virtual en el momento en que se crea la instantánea. El nombre de archivo usa la sintaxis `S1vm.snapshot1.vmsn`, donde `S1vm` corresponde al nombre de la máquina virtual y `snapshot1` corresponde a la primera instantánea. **Nota** Se genera un archivo `.vmsn` cada vez que se crea una instantánea, independientemente de la selección de memoria. Un archivo `.vmsn` sin memoria es mucho más pequeño que uno con memoria.

Limitaciones de las instantáneas

Las instantáneas pueden afectar el rendimiento de la máquina virtual y no son compatibles con ciertos tipos de discos o máquinas virtuales configuradas para uso compartido de bus. Las instantáneas son útiles como soluciones a corto plazo para la captura de los estados de las máquinas virtuales en un punto en el tiempo, pero no son adecuadas para copias de seguridad de máquinas virtuales a largo plazo.

- VMware no admite instantáneas de discos sin procesar, discos en modo físico de RDM ni sistemas operativos invitados que usan un iniciador iSCSI en el invitado.
- Las máquinas virtuales con discos independientes deben apagarse antes de la creación de una instantánea.
- Las instantáneas en modo inactivo requieren la instalación de VMware Tools y la compatibilidad con el sistema operativo invitado.
- Las instantáneas no son compatibles con dispositivos PCI de vSphere DirectPath I/O.
- VMware no admite instantáneas de máquinas virtuales configuradas para uso compartido de bus. Si requiere uso compartido de bus, considere la posibilidad de ejecutar un software de copia de seguridad en el sistema operativo invitado como solución alternativa. Si la máquina virtual actualmente tiene instantáneas que le impiden configurar el uso compartido de bus, elimine (consolide) las instantáneas.
- Las instantáneas proporcionan una imagen en un punto en el tiempo del disco que las soluciones de copia de seguridad pueden utilizar, pero no están diseñadas para usarse

como un método sólido de copia de seguridad y recuperación. Si los archivos que contienen una máquina virtual se pierden, sus archivos de instantáneas también se pierden. Además, las grandes cantidades de instantáneas son difíciles de administrar, consumen grandes cantidades de espacio de disco y no están protegidas contra errores de hardware.

- Las instantáneas pueden perjudicar el rendimiento de una máquina virtual. La degradación del rendimiento se basa en la cantidad de tiempo que se conservan la instantánea o el árbol de instantáneas, en la profundidad del árbol y en el grado de cambio que han experimentado la máquina virtual y su sistema operativo invitado desde el momento en que se creó la instantánea. Además, es posible que note un retraso en la cantidad de tiempo que la máquina virtual tarda en encender. No ejecute máquinas virtuales de producción a partir de instantáneas como una práctica permanente.
- Si una máquina virtual tiene discos duros virtuales que superan los 2 TB de capacidad, las operaciones de instantáneas pueden tardar mucho más tiempo en finalizar.

Crear snapshots de una máquina virtual

Puede crear una o más snapshots de una máquina virtual para crear el estado de la configuración, del disco y de la memoria a horas específicas. Al crear una snapshot, también puede poner los archivos de la máquina virtual en modo inactivo y excluir los discos de la máquina virtual de las snapshots.

Cuando se crea una snapshot, cualquier otra actividad que se esté realizando en la máquina virtual puede afectar al proceso de creación de la snapshot cuando se realice una reversión a la snapshot. El mejor momento para crear una snapshot, desde la perspectiva del almacenamiento, es cuando no está en ejecución ninguna carga importante de E/S. Desde la perspectiva del servicio, el mejor momento para crear una snapshot es cuando no hay aplicaciones en la máquina virtual que se comuniquen con otros equipos. La posibilidad de que se produzcan problemas es mayor si la máquina virtual se está comunicando con otro equipo, especialmente en un entorno de producción. Por ejemplo, si se crea una snapshot mientras la máquina virtual está descargando un archivo desde un servidor de la red, la máquina virtual sigue descargando el archivo y comunicando su progreso al servidor. Si se realiza una reversión a la snapshot, las comunicaciones entre la máquina virtual y el servidor se confunden, y se produce un error en la transferencia de los archivos. Según la tarea que se esté realizando, es posible volver a crear una snapshot de memoria o poner en modo inactivo el sistema de archivos en la máquina virtual.

Snapshots creadas con memoria

La selección predeterminada para la creación de snapshots. Cuando se captura el estado de la memoria de la máquina virtual, la snapshot retiene el estado activo de la máquina virtual. Las snapshots creadas con memoria realizan una snapshot en un momento preciso, por ejemplo, para actualizar software que aún está en funcionamiento. Si crea una snapshot de memoria y la actualización no finaliza de la manera esperada, o si el software no cumple con sus expectativas, puede realizar una reversión al estado anterior de la máquina virtual.

Cuando se captura el estado de la memoria, no es necesario poner en modo inactivo los archivos de la máquina virtual. Si no se captura el estado de la memoria, la snapshot no guarda el estado activo de la máquina virtual y los discos tienen coherencia ante fallos, a menos que se pongan en modo inactivo.

Snapshots en modo inactivo

Cuando se pone una máquina virtual en modo inactivo, VMware Tools pone en modo inactivo al sistema de archivos de la máquina virtual. Una operación de puesta en modo inactivo garantiza que el disco de la snapshot represente un estado coherente de los sistemas de archivo invitados. Las snapshots en modo inactivo resultan adecuadas para las copias de seguridad automatizadas o periódicas. Por ejemplo, si se desconoce la actividad de la máquina virtual, pero se desea disponer de varias copias de seguridad recientes para realizar reversiones, es posible poner los archivos en modo inactivo.

Si la máquina virtual está apagada o si VMware Tools no está disponible, el parámetro `Quiesce` (Poner en modo inactivo) no está disponible. Las máquinas virtuales que tienen discos de gran capacidad no se pueden poner en modo inactivo.

Importante No use las snapshots como su única solución de copia de seguridad ni como una solución de copia de seguridad a largo plazo.

Crear una instantánea en VMware Host Client

Las instantáneas capturan el estado completo de la máquina virtual en el momento en que se crea la instantánea. Puede crear una instantánea cuando se enciende, apaga o suspende una máquina virtual. Para crear una instantánea de una máquina virtual suspendida, espere hasta que la operación de suspensión termine antes de crear la instantánea.

Al crear una instantánea de memoria, la instantánea captura el estado de la memoria de la máquina virtual y la configuración de energía de la máquina virtual. Las instantáneas que capturan el estado de memoria de una máquina virtual tardan más en completarse. Es posible que también se advierta un retraso momentáneo en la respuesta a través de la red.

Al poner en modo inactivo una máquina virtual, VMware Tools inhabilita temporalmente el sistema de archivos en la máquina virtual. La operación de cambio a modo inactivo pausa o altera el estado de los procesos en ejecución en la máquina virtual, especialmente aquellos que pueden modificar la información que se almacena en el disco durante una operación de restauración.

No se admite el modo inactivo coherente con las aplicaciones en el caso de las máquinas virtuales con discos IDE o SATA.

Nota Si se toma una instantánea de un disco dinámico (tipo de disco específico de Microsoft), la tecnología de instantáneas conserva el estado de modo inactivo del sistema de archivos, pero no mantiene el estado de modo inactivo de la aplicación.

Requisitos previos

- Si desea capturar una instantánea de memoria de una máquina virtual que posee varios discos en diferentes nodos de disco, compruebe que la máquina virtual se encuentre apagada.
  Por ejemplo, si tiene una configuración de finalidad especial que le exige utilizar un disco independiente, debe apagar la máquina virtual antes de capturar una instantánea.
- Para capturar el estado de la memoria de la máquina virtual, compruebe que la máquina virtual esté encendida.
- Para poner en modo inactivo los archivos de la máquina virtual, compruebe que la máquina virtual esté encendida y que VMware Tools esté instalado.
- Compruebe si cuenta con el privilegio **Máquina virtual .Administración de instantáneas. Crear instantánea** en la máquina virtual.

Procedimiento

1. Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.
2. Haga clic con el botón derecho en una máquina virtual en la lista y seleccione **Instantáneas > Crear instantánea**.
3. Introduzca un nombre para la instantánea.
4. (opcional) Introduzca una descripción para la instantánea.
5. (opcional) Seleccione la casilla **Instantánea de la memoria de la máquina virtual** para capturar la memoria de la máquina virtual.
6. (opcional) Anule la selección de **Instantánea de la memoria de la máquina virtual** y seleccione la casilla **Poner en modo inactivo el sistema de archivos invitado (se requiere la instalación de VMware Tools)** para poner en pausa los procesos en ejecución en el sistema operativo invitado de forma tal que el contenido del sistema de archivos se encuentre en un estado coherente conocido cuando se cree la instantánea.

   Ponga en modo inactivo los archivos de la máquina virtual solamente cuando la máquina virtual esté encendida y no desee capturar el estado de la memoria de la máquina virtual.
7. Haga clic en **Crear instantánea**.

Restaurar snapshots

Para devolver una máquina virtual a su estado original o devolverla a otra snapshot en la jerarquía de snapshots, puede restaurar una snapshot.

Cuando se restaura una snapshot, la memoria de la máquina virtual, su configuración y los discos de la máquina virtual regresan al estado en que se encontraban en el momento en que tomó la snapshot. Si desea que una máquina virtual se suspenda, encienda o apague en el inicio, asegúrese de que esté en el estado correcto cuando cree la snapshot.

Puede restaurar instantáneas de las siguientes formas:

Revertir a la última instantánea

Restaura la instantánea primaria, un nivel hacia arriba en la jerarquía desde la posición **Usted está aquí**. **Revertir a la última instantánea** activa la instantánea primaria del estado actual de la máquina virtual.

Revertir a

Permite restaurar cualquier instantánea en el árbol de instantáneas y hace que esa instantánea sea la primaria del estado actual de la máquina virtual. Las instantáneas posteriores a partir de este punto crean una nueva rama del árbol de instantáneas.

La restauración de instantáneas tiene los siguientes efectos:

- Los estados actuales del disco y de la memoria se descartan, y la máquina virtual se revierte a los estados de disco y memoria correspondientes a la instantánea primaria.
- Las instantáneas existentes no se eliminan. Puede restaurar dichas instantáneas en cualquier momento.
- Si la instantánea incluye el estado de la memoria, la máquina virtual tendrá en el mismo estado de energía que cuando se creó la instantánea.

Tabla 3-4. Estado de energía de la máquina virtual después de restaurar una instantánea

Estado de la máquina virtual cuando se crea la instantánea primaria	Estado de la máquina virtual después de la restauración
Encendido (incluye memoria)	Revierte a la instantánea primaria, y la máquina virtual queda encendida y en ejecución.
Encendida (no incluye memoria)	Revierte a la instantánea primaria y la máquina virtual queda apagada.
Apagada (no incluye memoria)	Revierte a la instantánea primaria y la máquina virtual queda apagada.

Las máquinas virtuales que ejecutan ciertas cargas de trabajo pueden tardar varios minutos en reanudar la capacidad de respuesta después de realizar la reversión a partir de una instantánea.

Nota Los metadatos de vApp para máquinas virtuales en las vApps no siguen la semántica de la instantánea para configuración de máquinas virtuales. Las propiedades de vApp que se eliminan, modifican o definen después de que se crea una instantánea permanecen intactas (eliminadas, modificadas o definidas) después de que la máquina virtual se revierte a esa instantánea o a cualquier instantánea anterior.

Revertir a la instantánea más reciente en VMware Host Client

Realice una reversión a una instantánea para restaurar la máquina virtual al estado de la instantánea.

Requisitos previos

Verifique que posea el privilegio **Máquina virtual.Administrador de instantáneas.Revertir a instantánea** en la máquina virtual.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Haga clic con el botón derecho en la máquina virtual en la lista y seleccione **Instantáneas > Restaurar instantánea**.

Nota El estado actual de la máquina virtual se perderá a menos que lo guarde en una instantánea.

3 Haga clic en **Restaurar** para revertir la máquina virtual a la instantánea más reciente.

Eliminar snapshots

Al eliminar una snapshot, esta se quita del Administrador de snapshots. Los archivos de la snapshot se consolidan y escriben en el disco de snapshots primario. A continuación, se combinan con el disco base de la máquina virtual.

La eliminación de una instantánea no modifica la máquina virtual ni otras instantáneas. Al eliminar una instantánea, se consolidan los cambios entre las instantáneas y los estados de disco anteriores. Además, se escriben en el disco primario todos los datos del disco delta que contiene la información sobre la instantánea que se eliminó. Cuando elimina la instantánea primaria base, todos los cambios se combinan con el disco de la máquina virtual base.

Para eliminar una instantánea, es necesario leer y escribir gran cantidad de información en un disco. Este proceso puede disminuir el rendimiento de una máquina virtual hasta que finalice la consolidación. Con la consolidación de instantáneas se eliminan los discos redundantes, lo cual mejora el rendimiento de la máquina virtual y ahorra espacio de almacenamiento. El tiempo que se tarda en eliminar instantáneas y consolidar los archivos de estas depende de la cantidad de datos que el sistema operativo invitado escribe en los discos virtuales después de que se crea la última instantánea. Si la máquina virtual está encendida, el tiempo necesario es proporcional a la cantidad de datos que la máquina virtual escribe durante la consolidación.

El error en la consolidación de un disco merma el rendimiento de las máquinas virtuales. Puede ver una lista para comprobar si alguna máquina virtual requiere operaciones de consolidación separadas. Para obtener información sobre cómo encontrar y ver el estado de consolidación de varias máquinas virtuales, y sobre cómo ejecutar una operación de consolidación independiente, consulte *Administrar máquinas virtuales de vSphere*.

Eliminar

Utilice la opción **Eliminar** para eliminar una única instantánea primaria o secundaria del árbol de instantáneas. La opción **Eliminar** escribe los cambios del disco producidos entre el estado de la instantánea y el estado anterior del disco en la instantánea primaria.

Nota Al eliminar una sola instantánea, se conserva el estado actual de la máquina virtual y ninguna otra instantánea se ve afectada.

También puede utilizar la opción **Eliminar** para quitar una instantánea dañada y sus archivos de una rama abandonada del árbol de instantáneas sin combinarlos con la instantánea primaria.

Eliminar todo

Utilice la opción **Eliminar todo** para eliminar todas las instantáneas del Administrador de instantáneas. La opción **Eliminar todo** consolida y escribe los cambios producidos entre las instantáneas y los estados de disco delta anteriores en el disco primario base. Además, los combina con el disco de la máquina virtual base.

Para evitar que los archivos de instantáneas se combinen con la instantánea primaria (por ejemplo, si se produce un error en una operación de una actualización o instalación), primero use el comando **Restaurar** para realizar una restauración a una instantánea anterior. Esta acción invalida los discos delta de la instantánea y elimina el archivo de memoria. A continuación, puede utilizar la opción **Eliminar** para quitar la instantánea y los archivos asociados.

Eliminar una instantánea en VMware Host Client

Puede usar el administrador de instantáneas para eliminar una instantánea individual o todas las instantáneas de un árbol.

Tenga cuidado de no borrar accidentalmente una instantánea que necesite. No se pueden restaurar las instantáneas eliminadas. Por ejemplo, es posible que desee instalar varios exploradores (a, b y c) y capturar el estado de la máquina virtual después de la instalación de cada explorador. La primera instantánea, o instantánea de base, captura la máquina virtual con el explorador a y la segunda captura el explorador b. Si restaura la instantánea de base que incluye el explorador a y crea la tercera instantánea para capturar el explorador c y elimina la instantánea que incluye el explorador b, no podrá restaurar el estado de la máquina virtual que incluye el explorador b.

Procedimiento

1. Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.
2. Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Instantáneas > Administrar instantáneas**.
3. Haga clic en la instantánea que desee eliminar y, a continuación, haga clic en **Eliminar instantánea**.
4. (opcional) En el cuadro de diálogo **Eliminar instantánea**, seleccione la casilla **Eliminar todas las instantáneas secundarias** para quitar la instantánea seleccionada junto con todas sus instantáneas secundarias.
5. Haga clic en **Eliminar** para confirmar la eliminación.
6. Haga clic en **Cerrar** para salir del administrador de instantáneas.

Administrar instantáneas con VMware Host Client

Puede revisar todas las instantáneas de sus máquina virtuales y usar el administrador de instantáneas para administrarlas.

Después de crear una instantánea, puede hacer clic con el botón derecho en la máquina virtual y hacer clic en **Revertir a instantánea** para restaurar la máquina virtual al estado de la instantánea en cualquier momento.

Si tiene una serie de instantáneas, puede usar el administrador de instantáneas para restaurar cualquier instantánea primaria o secundaria. Las instantáneas secundarias posteriores que genere a partir de la instantánea restaurada crearán una rama en el árbol de instantáneas. Use el administrador de instantáneas para eliminar una instantánea del árbol.

Tabla 3-5. Administrador de instantáneas

Opción	Descripción
Árbol de instantáneas	Muestra todas las instantáneas de la máquina virtual.
Icono **Usted está aquí**	El icono **Usted está aquí** representa el estado actual y activo de la máquina virtual. Las acciones **Restaurar**, **Eliminar** y **Editar** están deshabilitadas para el estado **Usted está aquí**.
Tomar, **Restaurar**, **Eliminar**, **Editar**	Opciones de instantáneas.
Detalles	Muestra el nombre y la descripción de la instantánea, y la fecha de creación de la instantánea. La consola muestra el estado de energía que tenía la máquina virtual cuando se creó la instantánea. Los cuatros de texto Nombre, Descripción y Fecha de creación aparecen en blanco si no se selecciona una instantánea.

Supervisar una máquina virtual en VMware Host Client

Puede supervisar varios aspectos del rendimiento y realizar un seguimiento de las acciones que se ejecutan en las máquinas virtuales creadas en VMware Host Client.

Ver gráficos de rendimiento de máquinas virtuales en VMware Host Client

Puede ver gráficos de líneas con información acerca del uso de los recursos de las máquinas virtuales que crea en VMware Host Client.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Haga clic en una máquina virtual de la lista.

3 Expanda la máquina virtual en el inventario de VMware Host Client y haga clic en **Supervisar**.

4 Haga clic en **Rendimiento**.

5 Para ver el uso de los recursos de la máquina virtual durante la última hora, seleccione una opción en el menú desplegable.

- Para ver el porcentaje de CPU que usó la máquina virtual durante la última hora, seleccione **Uso de CPU**.
- Para ver la memoria que consumió el host durante la última hora, seleccione **Uso de memoria**.

Ver eventos de máquinas virtuales en VMware Host Client

Los eventos son registros de las acciones que un usuario realiza en una máquina virtual. Al crear una máquina virtual en VMware Host Client, podrá ver los eventos asociados con la máquina virtual.

Requisitos previos

Privilegio necesario: **Solo lectura**.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Haga clic en una máquina virtual de la lista.

3 Expanda la máquina virtual en el inventario de VMware Host Client y haga clic en **Supervisar**.

4 Haga clic en **Eventos**.

Se muestra una lista de todos los eventos de la máquina virtual.

5 (opcional) Haga clic en un evento de la lista para ver sus detalles.

6 (opcional) Para filtrar la lista, utilice los controles de filtro que se encuentran sobre la lista.

7 (opcional) Para ordenar la lista, haga clic en un encabezado de columna.

Ver tareas de máquinas virtuales en VMware Host Client

Al crear una máquina virtual en VMware Host Client, puede ver todas las tareas de la máquina virtual y la información acerca del destino de la tarea, el iniciador, el tiempo en cola, la hora de inicio, el resultado y la hora de finalización.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Haga clic en una máquina virtual de la lista.

3 Expanda la máquina virtual en el inventario de VMware Host Client y haga clic en **Supervisar**.

4 Haga clic en **Tareas**.

5 (opcional) Haga clic en una tarea de la lista para ver sus detalles.

6 (opcional) Para filtrar la lista, utilice los controles de filtro que se encuentran sobre la lista.

7 (opcional) Para ordenar la lista, haga clic en un encabezado de columna.

Ver el explorador de registros de máquinas virtuales en VMware Host Client

Genere y supervise registros para el host que está administrando mediante VMware Host Client. Use los registros para diagnosticar y solucionar diversos problemas en el entorno de host.

Procedimiento

1. Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.
2. Haga clic en una máquina virtual de la lista.
3. Expanda la máquina virtual en el inventario de VMware Host Client y haga clic en **Supervisar**.
4. Haga clic en **Registros**.
5. (opcional) Haga clic en **Generar paquete de soporte** para consolidar todos los registros para fines de solución de problemas.
6. Haga clic con el botón derecho en un registro de la lista y seleccione **Abrir en una ventana nueva** para ver el registro.

Ver notificaciones de máquinas virtuales en VMware Host Client

Puede ver notificaciones de las máquinas virtuales e información acerca de las tareas relacionadas, las cuales se pueden realizar para las máquinas virtuales creadas en VMware Host Client.

Procedimiento

1. Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.
2. Haga clic en una máquina virtual de la lista.
3. Expanda la máquina virtual en el inventario de VMware Host Client y haga clic en **Supervisar**.
4. Haga clic en **Notificaciones**.

   Se muestra una lista de todas las notificaciones de las máquinas virtuales.
5. (opcional) Haga clic en una notificación para ver sus detalles.
6. (opcional) Haga clic en una notificación y, a continuación, haga clic en **Acciones** para ver las tareas sugeridas.

Proteger las máquinas virtuales en VMware Host Client

El sistema operativo invitado que se ejecuta en la máquina virtual es vulnerable a los mismos riesgos de seguridad que un sistema físico. Para aumentar la seguridad del entorno virtual, puede agregar un módulo de plataforma de confianza (vTPM) virtual a los hosts ESXi. También puede habilitar la seguridad basada en virtualización (Virtualization-based Security, VBS) para las

máquinas virtuales que se ejecutan en los sistemas operativos Windows 10 y Windows Server 2016 más recientes.

Usar TPM virtual en VMware Host Client

El módulo TPM es un chip especializado que almacena información confidencial específica del host, como claves privadas e información confidencial del sistema operativo. El chip de TPM también se utiliza para realizar tareas de cifrado y dar fe de la integridad de la plataforma.

El dispositivo TPM virtual es una emulación de software de la funcionalidad TPM. Puede agregar un dispositivo TPM virtual (vTPM) a las máquinas virtuales del entorno. La implementación de vTPM no requiere un chip TPM físico en el host. ESXi utiliza el dispositivo vTPM para ejecutar la funcionalidad TPM en el entorno de vSphere.

vTPM está disponible para máquinas virtuales con sistemas operativos Windows 10 y Windows Server 2016. La máquina virtual debe tener la versión de hardware 14 o una posterior.

Puede agregar un dispositivo TPM virtual a una máquina virtual solo en la instancia de vCenter Server. Para obtener más información, consulte la documentación sobre *Seguridad de vSphere*.

En VMware Host Client, solo puede eliminar el dispositivo TPM virtual desde una máquina virtual.

Usar VBS en VMware Host Client

La seguridad basada en virtualización (Virtualization-based Security, VBS) utiliza la tecnología de virtualización basada en Microsoft Hyper-V para aislar los servicios básicos del sistema operativo Windows en otro entorno virtualizado. Este tipo de aislamiento proporciona un nivel adicional de protección, ya que hace imposible la manipulación de los servicios clave del entorno.

La habilitación automática de VBS en una máquina virtual activa el hardware virtual que Windows necesita para la función VBS. Al habilitar VBS, se inicia una variante de Hyper-V en la máquina virtual y Windows comienza a ejecutarse dentro de la partición raíz de Hyper-V.

VBS está disponible en las versiones más recientes de sistema operativo Windows, por ejemplo, Windows 10 y Windows Server 2016. Para utilizar VBS en una máquina virtual, debe tener compatibilidad con ESXi 6.7 y versiones posteriores.

En VMware Host Client, puede habilitar VBS durante la creación de la máquina virtual. Como alternativa, puede habilitar o deshabilitar VBS para una máquina virtual existente.

Nota VBS puede habilitarse en una máquina virtual solo si la validación de TPM del host se realiza correctamente.

Quitar un dispositivo vTPM de una máquina virtual en VMware Host Client

En VMware Host Client, solo se puede eliminar el dispositivo vTPM desde una máquina virtual.

Requisitos previos

- La máquina virtual debe tener la versión de hardware 14 o una posterior.

- El SO invitado debe ser Windows 10 o Windows Server 2016 y versiones posteriores.
- La máquina virtual debe estar apagada.

Procedimiento

1. Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.
2. Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Editar configuración** en el menú emergente.
3. En la pestaña **Hardware virtual**, busque el dispositivo TPM y haga clic en el icono **Quitar**.

   El dispositivo TPM virtual se elimina de la máquina virtual.
4. Haga clic en **Guardar** para cerrar el asistente.

Habilite o deshabilite la seguridad basada en la virtualización en una máquina virtual existente en el VMware Host Client

Puede habilitar la VBS de Microsoft en las máquinas virtuales existentes para sistemas operativos invitados Windows admitidos.

Requisitos previos

La habilitación de VBS es un proceso en el que primero se debe habilitar VBS en la máquina virtual y, posteriormente habilitar VBS en el sistema operativo invitado.

Nota Las máquinas virtuales nuevas configuradas para Windows 10, Windows Server 2016 y Windows Server 2019 en versiones de hardware inferiores a la versión 14 se deben crear mediante BIOS heredado de forma predeterminada. Si cambia el tipo de firmware de la máquina virtual de BIOS heredado a UEFI, debe volver a instalar el sistema operativo invitado.

Consulte la documentación de *vSphere Security* para obtener información sobre las prácticas recomendadas de CPU y VBS aceptables.

El uso de las CPU Intel para VBS requiere vSphere 6.7 o una versión posterior. La máquina virtual debe ser una creada con hardware de versión 14 o posterior y uno de los siguientes sistemas operativos invitados compatibles:

- Windows 10 (64 bits) o versiones posteriores
- Windows Server 2016 (64 bits) o versiones posteriores

El uso de las CPU AMD para VBS requiere vSphere 7.0 Update 2 o una versión posterior. La máquina virtual debe ser una creada con hardware de versión 19 o posterior y uno de los siguientes sistemas operativos invitados compatibles:

- Windows 10 (64 bits), versión 1809 o versiones posteriores
- Windows Server 2019 (64 bits) o versiones posteriores

Antes de habilitar VBS, asegúrese de instalar las revisiones más recientes para Windows 10, versión 1809 y Windows Server 2019.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.

2 Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Editar configuración** en el menú emergente.

3 En la pestaña **Opciones de máquina virtual**, habilite o deshabilite VBS para la máquina virtual.

   - Para habilitar VBS para la máquina virtual, active la casilla **Habilitar seguridad basada en virtualización**.
   - Para deshabilitar VBS en la máquina virtual, desactive la casilla **Habilitar seguridad basada en virtualización**.

   Al habilitar VBS, varias opciones se seleccionan automáticamente y se atenúan en el asistente.

4 Haga clic en **Guardar** para cerrar el asistente.

Administrar almacenamiento en VMware Host Client

4

Al conectarse a un host ESXi mediante VMware Host Client, puede realizar diferentes tareas de administración de almacenamiento en el host ESXi, entre ellas, configurar adaptadores, crear almacenes de datos y ver información de dispositivos de almacenamiento.

Este capítulo incluye los siguientes temas:

Trabajar con almacenes de datos en VMware Host Client

Los almacenes de datos son contenedores lógicos, similares a los sistemas de archivos, que contienen aspectos específicos de cada dispositivo de almacenamiento y ofrecen un modelo uniforme para almacenar archivos de máquinas virtuales. Los almacenes de datos también pueden utilizarse para almacenar imágenes ISO, plantillas de máquinas virtuales e imágenes de disquete.

Según el tipo de almacenamiento que se utilice, los almacenes de datos pueden ser de los siguientes tipos:

- Virtual Machine File System (VMFS)
- Network File System (NFS)

Puede aumentar la capacidad de un almacén de datos después de crearlo, pero solamente si se trata de un almacén de datos de VMFS.

Ver información de almacenes de datos en VMware Host Client

Utilice VMware Host Client para mostrar los almacenes de datos a disposición de los hosts, y analice sus propiedades.

Procedimiento

1 Haga clic en **Almacenamiento** en el inventario de VMware Host Client y, a continuación, haga clic en **Almacenes de datos**.

2 Para ver los detalles de un almacén de datos específico, seleccione el almacén de datos de la lista.

Crear un almacén de datos de VMFS en VMware Host Client

Los almacenes de datos de VMFS sirven como repositorios para las máquinas virtuales. Los almacenes de datos de VMFS se pueden configurar en cualquier dispositivo de almacenamiento basado en SCSI que el host detecte, incluidos los dispositivos de almacenamiento locales, iSCSI y de canal de fibra. Puede utilizar el asistente **Nuevo almacén de datos** para crear un almacén de datos en VMware Host Client.

Requisitos previos

Instale y configure todos los adaptadores que requiere el almacenamiento. Vuelva a examinar los adaptadores para detectar los dispositivos de almacenamiento recientemente agregados.

Procedimiento

1 Haga clic en **Almacenamiento** en el inventario de VMware Host Client y, a continuación, haga clic en **Almacenes de datos**.

2 Haga clic en **Nuevo almacén de datos**.

   Se abre el asistente **Nuevo almacén de datos**.

3 En la página Seleccionar tipo de creación, elija **Crear nuevo almacén de datos de VMFS** y haga clic en **Siguiente**.

Opción	Descripción
Crear nuevo almacén de datos de VMFS	Crea un nuevo almacén de datos de VMFS en un dispositivo de disco local.
Agregar una extensión al almacén de datos de VMFS existente	Aumenta el tamaño de un almacén de datos existente agregando una nueva extensión en otro disco.
Ampliar una extensión del almacén de datos de VMFS existente	Aumenta el tamaño del alcance de un almacén de datos existente.
Montar almacén de datos de NFS	Crea un nuevo almacén de datos montando un volumen NFS remoto.

4 En la página Seleccionar dispositivo, elija dónde desea crear la nueva partición VMFS.

   a Introduzca un nombre para el almacén de datos.

   b Seleccione un dispositivo donde agregar el almacén de datos.

      La lista contiene solamente los dispositivos que poseen suficiente espacio disponible.

   c Haga clic en **Siguiente**.

5 En la página Seleccionar opciones de partición, seleccione la forma en que desea particionar el dispositivo y haga clic en **Siguiente**.

Opción	Descripción
Uso del disco completo	Muestra todo el espacio libre que está disponible en el dispositivo.
Personalizado	Haga clic en la barra **Espacio libre** y use el control deslizante horizontal para particionar el dispositivo.

6 En la página Listo para completar, revise los detalles de configuración y haga clic en **Finalizar**.

Aumentar la capacidad de un almacén de datos de VMFS

Si el almacén de datos de VMFS requiere más espacio, aumente la capacidad del almacén de datos. Puede aumentar la capacidad dinámicamente si amplía una extensión del almacén de datos o agrega una extensión.

Utilice uno de los siguientes métodos para aumentar la capacidad del almacén de datos:

- Amplíe dinámicamente cualquier extensión de almacén de datos expandible para llenar la capacidad adyacente disponible. La extensión se considera expandible cuando el dispositivo de almacenamiento subyacente tiene espacio libre inmediatamente después de la extensión.
- Agregue la extensión dinámicamente. El almacén de datos puede expandir un máximo de 32 extensiones, con un tamaño superior a 2 TB cada una, y seguir apareciendo como un solo volumen. El almacén de datos de VMFS expandido puede utilizar cualquiera de las extensiones o todas ellas en cualquier momento. No es necesario que complete una extensión en especial para poder utilizar la siguiente.

Nota Los almacenes de datos que admiten solo bloqueo asistido por hardware, también denominado mecanismo ATS, no pueden expandirse a dispositivos sin bloqueo con ATS. Para obtener más información, consulte *Almacenamiento de vSphere*.

Ampliar un almacén de datos de VMFS existente en VMware Host Client

Cuando necesita agregar máquinas virtuales a un almacén de datos o cuando las máquinas virtuales que se ejecutan en un almacén de datos requieren más espacio, puede aumentar dinámicamente la capacidad de un almacén de datos de VMFS.

Si un almacén de datos encendió máquinas virtuales y se completa al 100%, puede aumentar la capacidad del almacén de datos solo desde el host con el que están registradas las máquinas virtuales encendidas.

Procedimiento

1 Haga clic en **Almacenamiento** en el inventario de VMware Host Client y, a continuación, haga clic en **Almacenes de datos**.

2 Haga clic en **Nuevo almacén de datos**.

3 En la página Seleccionar tipo de creación, haga clic en **Agregar una extensión al almacén de datos de VMFS existente** y haga clic en **Siguiente**.

4 En la página Seleccionar almacén de datos, seleccione el almacén de datos que desea expandir y haga clic en **Siguiente**.

5 En la página Seleccionar dispositivo, seleccione el dispositivo en el que desea crear la nueva partición VMFS y haga clic en **Siguiente**.

6 En la página Seleccionar opciones de partición, seleccione la forma en que desea particionar el dispositivo y haga clic en **Siguiente**.

Opción	Descripción
Uso del disco completo	Muestra todo el espacio libre que está disponible en el dispositivo.
Personalizado	Haga clic en la barra **Espacio libre** y use el control deslizante horizontal para particionar el dispositivo.

7 En la página Listo para completar, revise los detalles de configuración y haga clic en **Finalizar**.

Montar un almacén de datos de Network File System en el VMware Host Client

Con VMware Host Client, puede crear un almacén de datos NFS (Network File System) para almacenar discos virtuales y para usarlo como repositorio central de imágenes ISO, máquinas virtuales, etc. Un cliente NFS integrado en ESXi utiliza el protocolo Network File System (NFS) mediante TCP/IP para acceder a un volumen NFS designado ubicado en un servidor NAS. vSphere es compatible con las versiones 3 y 4.1 del protocolo NFS.

El host ESXi puede montar un volumen NFS y utilizarlo para sus necesidades de almacenamiento.

En general, un administrador de almacenamiento crea el directorio o el volumen NFS, y este se exporta del servidor NFS. No es necesario dar formato al volumen NFS con un sistema de archivos local, como VMFS. En cambio, se debe montar el volumen directamente en los hosts ESXi y utilizarlo para almacenar y arrancar máquinas virtuales del mismo modo en que se utilizan los almacenes de datos de VMFS.

Además de almacenar discos virtuales en almacenes de datos NFS, se puede utilizar NFS como un repositorio central de imágenes ISO, plantillas de máquina virtual, etc. Si utiliza el almacén de datos para las imágenes ISO, puede conectar el dispositivo de CD-ROM de la máquina virtual a un archivo ISO en el almacén de datos. Luego, puede instalar un sistema operativo invitado desde el archivo ISO.

Al utilizar el almacenamiento NFS, siga las directrices específicas para la configuración del servidor NFS, las redes, los almacenes de datos NFS, etc.

Procedimiento

1 Montar un almacén de datos NFS en VMware Host Client

   Use el asistente **Nuevo almacén de datos** para montar un almacén de datos NFS (Network File System) en VMware Host Client.

Montar un almacén de datos NFS en VMware Host Client

Use el asistente **Nuevo almacén de datos** para montar un almacén de datos NFS (Network File System) en VMware Host Client.

Requisitos previos

Como NFS requiere conectividad de red para acceder a los datos almacenados en servidores remotos, antes de configurar NFS, debe configurar las redes VMkernel.

Procedimiento

1 Haga clic en **Almacenamiento** en el inventario de VMware Host Client y, a continuación, haga clic en **Almacenes de datos**.

2 Haga clic en **Nuevo almacén de datos**.

   Se abre el asistente **Nuevo almacén de datos**.

3 En la página Seleccionar tipo de creación, haga clic en **Montar almacén de datos de NFS** y haga clic en **Siguiente**.

4 En la página Proporcionar detalles del montaje de NFS, proporcione la información del NFS que desea montar.

   a Introduzca un nombre para el almacén de datos NFS.

   b Introduzca el nombre del servidor NFS.

      Para el nombre del servidor, puede introducir una dirección IP, un nombre DNS o un UUID de NFS.

      Nota Al montar el mismo volumen NFS en diferentes hosts, compruebe que los nombres de servidor y carpeta sean idénticos en todos los hosts. Si los nombres no coinciden, los hosts detectarán el mismo volumen NFS como dos almacenes de datos diferentes. Esto puede provocar que características como vMotion no funcionen correctamente. Por ejemplo, esta discrepancia se produce si se introduce `archivo` como nombre del servidor en un host y `archivo.dominio.com` en el otro.

   c Especifique el recurso compartido NFS.

   d Especifique la versión de NFS.

   e Haga clic en **Siguiente**.

5 En la página Listo para finalizar, revise las opciones de configuración para el almacén de datos NFS y haga clic en **Finalizar**.

Desmontar un almacén de datos en VMware Host Client

Al desmontar un almacén de datos en VMware Host Client, el almacén de datos permanece intacto, pero ya no se puede ver en el inventario del host que administra. El almacén de datos sigue apareciendo en los demás hosts en los que permanece montado.

No realice ninguna operación de configuración que pueda provocar operaciones de E/S en el almacén de datos mientras el desmontaje está en curso.

Requisitos previos

Nota Asegúrese de que los latidos de vSphere HA no usen el almacén de datos. Los latidos de vSphere HA no le impiden desmontar el almacén de datos. Sin embargo, si el almacén de datos se utiliza para los latidos, desmontarlo puede provocar que el host genere errores y reinicie todas las máquinas virtuales activas.

Antes de desmontar un almacén de datos, asegúrese de que se cumplan los siguientes requisitos previos:

- Ninguna máquina virtual debe residir en el almacén de datos.
- Storage DRS no administra el almacén de datos.
- Storage I/O Control debe estar deshabilitado para este almacén de datos.

Procedimiento

1 Haga clic en **Almacenamiento** en el inventario de VMware Host Client y, a continuación, haga clic en **Almacenes de datos**.

2 Haga clic con el botón derecho en el almacén de datos para desmontarlo de la lista y, a continuación, haga clic en **Desmontar**.

3 Confirme que desea desmontar el almacén de datos.

Errores en el desmontaje o la eliminación de un almacén de datos

Cuando se intenta desmontar o eliminar un almacén de datos, se produce un error en la operación.

Problema

Se produce un error en la operación para desmontar o eliminar un almacén de datos si el almacén de datos tiene archivos abiertos. Para estas operaciones de usuarios, el agente de vSphere HA cierra todos los archivos que tiene abiertos, por ejemplo archivos de latido. Si vCenter Server no puede acceder al agente o el agente no puede purgar E/S pendientes para cerrar los archivos, se acciona el error `El agente de HA en el host '{hostName}' presentó error al poner en modo inactivo la actividad del archivo en el almacén de datos {dsName}.`

Causa

Si el almacén de datos que se va a desmontar o eliminar se utiliza para verificación de latidos, vCenter Server lo excluye de la verificación de latidos y selecciona uno nuevo. Sin embargo, el agente no recibe los almacenes de datos con latido actualizado si no se puede acceder a él, es decir, si el host está aislado o en una partición de red. En dichos casos, los archivos de latido no se cierran y se produce un error de operación de usuario. La operación también puede presentar error si no se puede acceder al almacén de datos debido a errores de almacenamiento, como caída de todas las rutas de acceso.

Nota Cuando elimina un almacén de datos de VMFS, este almacén se quita de todos los hosts en el inventario. Por lo tanto, si hay hosts en un clúster de vSphere HA a los que no se puede acceder o que no tienen acceso al almacén de datos, hay error en la operación.

Solución

Asegúrese de que el almacén de datos esté accesible y que se pueda acceder a los hosts afectados.

Usar un explorador de archivos de almacenes de datos en VMware Host Client

Utilice el explorador de archivos del almacén de datos para administrar el contenido de su almacén de datos. Puede realizar diversas tareas, entre ellas, cargar archivos al almacén de datos, descargar archivos del almacén de datos en su sistema, mover y copiar carpetas y archivos del almacén de datos, y crear nuevos directorios de almacenes de datos.

Cargar archivos a un almacén de datos en VMware Host Client

Use el explorador de archivos de almacenes de datos para cargar archivos a almacenes de datos en su host.

Nota Virtual Volumes no admite la carga de archivos directa a los almacenes de datos virtuales. Primero se debe crear una carpeta en el almacén de datos virtual para después poder cargar los archivos en la carpeta.

Además de su uso tradicional como almacenamiento para archivos de máquinas virtuales, los almacenes de datos pueden servir para almacenar datos o archivos relacionados con máquinas virtuales. Por ejemplo, puede cargar imágenes ISO de sistemas operativos desde un equipo local a un almacén de datos en el host. A continuación, puede usar esas imágenes para instalar sistemas operativos invitados en las máquinas virtuales nuevas.

Requisitos previos

Privilegio necesario: **Almacén de datos.Examinar almacén de datos**

Procedimiento

1 Haga clic en **Almacenamiento** en el inventario de VMware Host Client y, a continuación, haga clic en **Almacenes de datos**.

2 Haga clic en **Explorador de almacenes de datos**.

3 Seleccione el almacén de datos en el que desee almacenar el archivo.

4 (opcional) Haga clic en **Crear directorio** para crear un nuevo directorio de almacén de datos donde almacenar el archivo.

5 Seleccione la carpeta de destino y haga clic en **Cargar**.

6 Ubique el elemento que desee cargar en el equipo local y haga clic en **Abrir**.

   El archivo se carga al almacén de datos que seleccionó.

7 (opcional) Actualice el explorador de archivos del almacén de datos para ver el archivo cargado en la lista.

8 Haga clic en **Cerrar** para salir del explorador de archivos.

Descargar archivos de un almacén de datos a su sistema en VMware Host Client

Use el explorador de archivos de almacenes de datos de los almacenes de datos disponibles en el host que está administrando en el sistema local.

Requisitos previos

Privilegio necesario: **Almacén de datos.Examinar almacén de datos**

Procedimiento

1 Haga clic en **Almacenamiento** en el inventario de VMware Host Client y, a continuación, haga clic en **Almacenes de datos**.

2 Haga clic en **Explorador de almacenes de datos**.

3 Seleccione el almacén de datos de destino.

4 Haga clic en la carpeta que contiene el archivo que desea descargar.

   Se muestran los archivos que están disponibles en la carpeta.

5 Haga clic en el archivo que desee descargar.

6 Haga clic en **Descargar**.

   El archivo se descarga en su sistema.

7 Haga clic en **Cerrar** para salir del explorador de archivos.

Eliminar archivos de un almacén de datos en VMware Host Client

Puede eliminar archivos de forma permanente de cualquier almacén de datos en caso que ya no los necesite.

Requisitos previos

Privilegio necesario: **Almacén de datos.Examinar almacén de datos**

Procedimiento

1 Haga clic en **Almacenamiento** en el inventario de VMware Host Client y, a continuación, haga clic en **Almacenes de datos**.
2 Haga clic en **Explorador de almacenes de datos**.
3 Seleccione el almacén de datos de destino.
4 Seleccione la carpeta que contiene el archivo que desea eliminar.

   Se muestran los archivos que están disponibles en la carpeta.
5 Haga clic en el archivo que desee eliminar del almacén de datos, luego en **Eliminar** y, por último, una vez más en **Eliminar**.
6 Haga clic en **Cerrar** para salir del explorador de archivos.

Mover archivos o carpetas de almacenes de datos en VMware Host Client

Utilice el explorador de archivos de almacenes de datos para mover carpetas o archivos a una ubicación nueva, ya sea en el mismo almacén de datos o en uno diferente.

Nota Los archivos de discos virtuales se mueven y se copian sin conversión de formato. Si mueve un disco virtual a un almacén de datos en un tipo diferente de host al tipo de host de origen, es posible que deba convertir los discos virtuales antes de utilizarlos.

Requisitos previos

Privilegio necesario: **Almacén de datos.Examinar almacén de datos**

Procedimiento

1 Haga clic en **Almacenamiento** en el inventario de VMware Host Client y, a continuación, haga clic en **Almacenes de datos**.
2 Haga clic en **Explorador de almacenes de datos**.
3 Seleccione el almacén de datos de destino.
4 Seleccione el archivo o la carpeta que desee mover a otra ubicación y haga clic en **Mover**.
5 Seleccione el destino y haga clic en **Mover**.
6 Haga clic en **Cerrar** para salir del explorador de archivos.

Copiar archivos o carpetas de almacenes de datos en VMware Host Client

Utilice el explorador de archivos del almacén de datos para copiar archivos o carpetas a una nueva ubicación en el mismo almacén de datos o en otro.

Nota Los archivos de discos virtuales se mueven y se copian sin conversión de formato. Si mueve un disco virtual a un almacén de datos en un tipo diferente de host al tipo de host de origen, posiblemente deba convertir los discos virtuales.

Requisitos previos

Privilegio necesario: **Almacén de datos.Examinar almacén de datos**

Procedimiento

1 Haga clic en **Almacenamiento** en el inventario de VMware Host Client y, a continuación, haga clic en **Almacenes de datos**.
2 Haga clic en **Explorador de almacenes de datos**.
3 Seleccione el almacén de datos de destino.
4 Seleccione el archivo o la carpeta que desee mover a otra ubicación y haga clic en **Copiar**.
5 Seleccione el destino y haga clic en **Copiar**.
6 Haga clic en **Cerrar** para salir del explorador de archivos.

Crear un nuevo directorio de almacenes de datos en VMware Host Client

Puede crear nuevos directorios de almacenes de datos si desea almacenar archivos en una ubicación en particular.

Requisitos previos

Privilegio necesario: **Almacén de datos.Examinar almacén de datos**

Procedimiento

1 Haga clic en **Almacenamiento** en el inventario de VMware Host Client y, a continuación, haga clic en **Almacenes de datos**.
2 Haga clic en **Explorador de almacenes de datos**.
3 Haga clic en **Crear directorio**.
4 Seleccione el almacén de datos de destino.
5 (opcional) Introduzca un nombre para el nuevo directorio.
6 Haga clic en **Crear directorio**.
7 Haga clic en **Cerrar** para salir del explorador de archivos.

Renombrar un almacén de datos en VMware Host Client

Se puede cambiar el nombre para mostrar de un almacén de datos en VMware Host Client.

Nota Si el host está administrado por vCenter Server, no se puede cambiar el nombre del almacén de datos desde VMware Host Client. Esta tarea solo se puede realizar desde la instancia de vCenter Server que administra el host.

Procedimiento

1 Haga clic en **Almacenamiento** en el inventario de VMware Host Client y, a continuación, haga clic en **Almacenes de datos**.

2 Haga clic con el botón derecho en el almacén de datos de la lista y seleccione **Cambiar nombre** en el menú desplegable.

3 Introduzca un nuevo nombre para el almacén de datos y haga clic en **Guardar** para aplicar los cambios.

4 (opcional) Haga clic en **Actualizar** para ver el nuevo nombre del almacén de datos en la lista de almacenes de datos disponibles.

Eliminar un almacén de datos de VMFS en VMware Host Client

Se puede eliminar cualquier tipo de almacén de datos de VMFS, incluidas las copias que se hayan montado sin volver a firmar. Al eliminar un almacén de datos, se eliminan del host todos los archivos y los datos asociados con dicho almacén de datos.

Nota La operación de eliminación del almacén de datos elimina de manera permanente todos los archivos asociados a las máquinas virtuales en el almacén de datos. Aunque es posible eliminar el almacén de datos sin necesidad de desmontar, es preferible que primero se desmonte el almacén de datos.

Requisitos previos

Quite todas las máquinas virtuales del almacén de datos.

Procedimiento

1 Haga clic en **Almacenamiento** en el inventario de VMware Host Client y, a continuación, haga clic en **Almacenes de datos**.

2 Haga clic con el botón derecho en el almacén de datos de la lista y seleccione **Eliminar** en el menú desplegable.

3 Haga clic en **Confirmar** para eliminar el almacén de datos.

Aceleración de hardware de almacenamiento

La funcionalidad de aceleración de hardware permite que el host ESXi se integre con sistemas de almacenamiento compatibles. El host puede descargar ciertas operaciones de administración

de máquina virtual y almacenamiento en los sistemas de almacenamiento. Con la asistencia de hardware de almacenamiento, el host realiza estas operaciones más rápidamente y consume menos CPU, memoria y ancho de banda de tejido de almacenamiento.

Los dispositivos de almacenamiento en bloque, canal de fibra y de iSCSI, y los dispositivos NAS admiten la aceleración de hardware.

Para obtener detalles adicionales, consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/1021976.

Deshabilitar la aceleración de hardware para dispositivos de almacenamiento en bloque en VMware Host Client

La aceleración del hardware del host para dispositivos de almacenamiento en bloque está habilitada de forma predeterminada en todos los hosts. Se puede utilizar la configuración avanzada de VMware Host Client para deshabilitar la aceleración de hardware.

No se admite la modificación de opciones de configuración avanzadas a menos que el soporte técnico de VMware le indique hacerlo.

Requisitos previos

Apague la máquina virtual.

Procedimiento

1 Haga clic en **Máquinas virtuales** en el inventario de VMware Host Client.
2 Haga clic con el botón derecho en la máquina virtual de la lista y seleccione **Editar configuración** en el menú desplegable.
3 En la pestaña **Opciones de máquina virtual**, expanda **Opciones avanzadas**.
4 En **Configuración**, seleccione **Deshabilitar aceleración**.
5 Haga clic en **Guardar**.

Aprovisionamiento fino de almacenamiento en VMware Host Client

Con ESXi, puede utilizar dos modelos de aprovisionamiento fino, en el nivel de la matriz y en el nivel del disco virtual.

El aprovisionamiento fino es un método que optimiza la utilización del almacenamiento mediante la asignación del espacio de almacenamiento de forma flexible y a pedido. El aprovisionamiento fino se contrapone al modelo tradicional, llamado aprovisionamiento grueso. Con el aprovisionamiento grueso, se proporciona por adelantado una gran cantidad de espacio de almacenamiento para anticipar necesidades de almacenamiento futuras. Sin embargo, el espacio puede permanecer inutilizado, lo que genera la infrautilización de la capacidad de almacenamiento.

Las características de aprovisionamiento fino de VMware ayudan a eliminar los problemas de infrautilización del almacenamiento en el nivel de la matriz de almacenamiento y del almacén de datos.

Crear discos virtuales de aprovisionamiento fino en VMware Host Client

Para ahorrar espacio de almacenamiento, puede crear discos virtuales con aprovisionamiento fino. El disco virtual con aprovisionamiento fino que se crea es pequeño y aumenta a medida que se requiere más espacio en disco. Es posible crear discos finos únicamente en almacenes de datos compatibles con aprovisionamiento fino en el nivel de disco.

El siguiente procedimiento da por sentado que se está creando una máquina virtual nueva. Para obtener más información, consulte Crear una máquina virtual en VMware Host Client.

Procedimiento

1 Haga clic con el botón derecho en **Host** desde el inventario de VMware Host Client y seleccione **Crear/Registrar máquina virtual**.

   Se abre el asistente **Nueva máquina virtual**.

2 Seleccione un método para agregar una nueva máquina virtual en el host y haga clic en **Siguiente**.

3 Introduzca un nombre para la máquina virtual.

4 Seleccione la compatibilidad de la máquina virtual en el menú desplegable **Compatibilidad**.

5 Seleccione una versión de sistema operativo invitado en el menú desplegable **Versión del sistema operativo invitado** y haga clic en **Siguiente**.

6 Desde la lista de almacenes accesibles en la página Seleccionar almacenamiento del asistente **Nueva máquina virtual**, seleccione el almacén de datos de destino para los archivos de configuración de la máquina virtual y para todos los discos virtuales.

7 En la pestaña **Hardware virtual**, expanda la opción **Disco duro**.

8 En **Aprovisionamiento de disco**, seleccione el botón de opción **Aprovisionamiento fino** y haga clic en **Siguiente**.

9 En la página Listo para finalizar del asistente **Nueva máquina virtual**, revise las opciones de configuración de la máquina virtual y haga clic en **Finalizar** para guardar la configuración.

Ver los recursos de almacenamiento de una máquina virtual en VMware Host Client

Es posible ver cómo el espacio de almacenamiento del almacén de datos se asigna a las máquinas virtuales en VMware Host Client.

Consumo de recursos muestra cuánto espacio del almacén de datos ocupan los archivos de la máquina virtual, incluidos los archivos de registro y configuración, las instantáneas, los discos virtuales, etc. Cuando la máquina virtual está en ejecución, el espacio de almacenamiento utilizado también incluye archivos de intercambio.

En las máquinas virtuales con discos finos, el valor de uso del almacenamiento real puede ser inferior al tamaño del disco virtual.

Procedimiento

1 Haga clic en la máquina virtual desde el inventario de VMware Host Client.

2 Revise la información de consumo de recursos en el área inferior derecha de la página de resumen de la máquina virtual.

Determinar el formato de disco de una máquina virtual en VMware Host Client

Puede determinar si el disco virtual está aprovisionado en formato grueso o fino.

Procedimiento

1 Haga clic con el botón derecho en una máquina virtual desde el inventario de VMware Host Client y seleccione **Editar configuración**.

2 En la pestaña **Hardware virtual**, expanda la opción **Disco duro**.

   El cuadro de texto **Tipo** muestra el formato del disco virtual.

Administrar adaptadores de almacenamiento en VMware Host Client

Cuando se conecta a un host o a vCenter Server a través de VMware Host Client, puede realizar diversas tareas en los adaptadores de almacenamiento, como configurar varios componentes de iSCSI.

Si habilita iSCSI en el host que está administrando en el entorno de VMware Host Client, puede configurar y agregar nuevos enlaces de puertos de red y destinos estáticos y dinámicos, administrar la autenticación CHAP y configurar diversos ajustes avanzados en el almacenamiento del host.

Ver adaptadores de almacenamiento en VMware Host Client

Vea los adaptadores de almacenamiento que usa su host y también la información relacionada.

Procedimiento

1 Haga clic en **Almacenamiento** desde el inventario de VMware Host Client y, a continuación, haga clic en **Adaptadores**.

   Todos los adaptadores de almacenamiento disponibles para el host se enumeran en **Adaptadores**.

2 Para ver los detalles de un adaptador específico, seleccione el adaptador en la lista.

Configurar los adaptadores de iSCSI de software en VMware Host Client

La implementación de iSCSI basado en software permite utilizar NIC estándar para conectar el host a un destino iSCSI remoto en la red IP. El adaptador de iSCSI de software incorporado en ESXi se comunica con las NIC físicas a través de la pila de red.

Nota Para poder utilizar el adaptador de iSCSI de software, debe configurar las redes, activar el adaptador y configurar parámetros como CHAP.

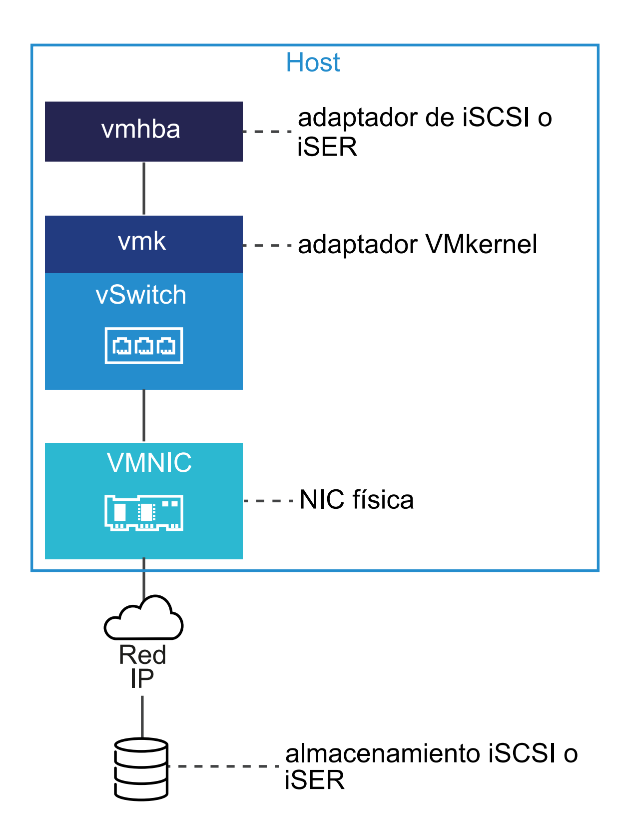
El flujo de trabajo de configuración del adaptador de iSCSI incluye los siguientes procedimientos:

- Habilitar iSCSI en el host. Consulte Habilitar iSCSI para un host ESXi en VMware Host Client.
- Agregar un enlace de puertos. Consulte Agregar enlaces de puertos en VMware Host Client.
- Eliminar el enlace de puertos. Consulte Quitar enlaces de puertos en VMware Host Client.

Configurar la seguridad de red para iSCSI e iSER

Ciertos tipos de adaptadores de iSCSI dependen de las redes de VMkernel. Estos adaptadores incluyen los adaptadores de iSCSI de hardware o de software dependiente y el iSCSI de VMware a través del adaptador RDMA (iSER). Si su entorno incluye alguno de estos adaptadores, debe configurar las conexiones para el tráfico entre el componente de iSCSI o iSER y los adaptadores de red física.

La configuración de la conexión de red implica la creación de un adaptador VMkernel virtual para cada adaptador de red físico. Use una asignación 1:1 entre cada adaptador de red física y virtual. A continuación, asocie el adaptador de VMkernel con un adaptador de iSCSI o iSER adecuado. Este proceso se conoce como enlace de puertos.



Siga estas reglas al configurar el enlace de puertos:

- Puede conectar el adaptador de iSCSI de software con cualquier NIC física disponible en el host.
- Los adaptadores de iSCSI dependientes deben estar conectados solo a sus propias NIC físicas.
- Debe conectar el adaptador de iSER solo con el adaptador de red compatible con RDMA.

Para observar las consideraciones específicas sobre cuándo y cómo utilizar las conexiones de red con iSCSI de software, consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/2038869.

Habilitar iSCSI para un host ESXi en VMware Host Client

Habilite iSCSI en el host del entorno de VMware Host Client para configurar los parámetros de los adaptadores de almacenamiento, como la autenticación CHAP, los enlaces de puertos de red, los destinos estáticos y dinámicos, y otras configuraciones avanzadas.

Procedimiento

1. Haga clic en **Almacenamiento** desde el inventario de VMware Host Client, luego en **Adaptadores** y, por último, en **Configurar iSCSI**.
2. Seleccione el botón de opción **Habilitado**.
3. (opcional) Configure los parámetros y componentes que desee modificar.
4. Haga clic en **Guardar configuración**.

Prácticas recomendadas para configurar redes con iSCSI de software

Al configurar redes con iSCSI de software, tenga en cuenta las distintas prácticas recomendadas.

Enlace de puertos iSCSI de software

Puede enlazar el iniciador de iSCSI de software en el host ESXi con un único o varios puertos de VMkernel, de modo que el tráfico de iSCSI circule solamente mediante los puertos enlazados. Para el tráfico iSCSI no se utilizan puertos sin enlazar.

Cuando se configura el enlace de puertos, el iniciador de iSCSI crea sesiones iSCSI desde todos los puertos enlazados hasta todos los portales de destino configurados.

Vea los siguientes ejemplos.

Puertos de VMkernel	Portales de destino	Sesiones iSCSI
2 puertos de VMkernel enlazados	2 portales de destino	4 sesiones (2 x 2)
4 puertos de VMkernel enlazados	1 portal de destino	4 sesiones (4 x 1)
2 puertos de VMkernel enlazados	4 portales de destino	8 sesiones (2 x 4)

Nota Al utilizar el enlace de puertos, asegúrese de que todos los portales de destino sean accesibles desde todos los puertos de VMkernel. De lo contrario, es posible que las sesiones iSCSI no puedan crearse. Como resultado, puede que la operación de reexaminación demore más de lo esperado.

Sin enlace de puertos

Si no usa el enlace de puertos, la capa de redes de ESXi selecciona el mejor puerto de VMkernel en función de su tabla de enrutamiento. El host usa el puerto para crear una sesión iSCSI en el portal de destino. Sin el enlace de puertos, solo se crea una sesión por cada portal de destino.

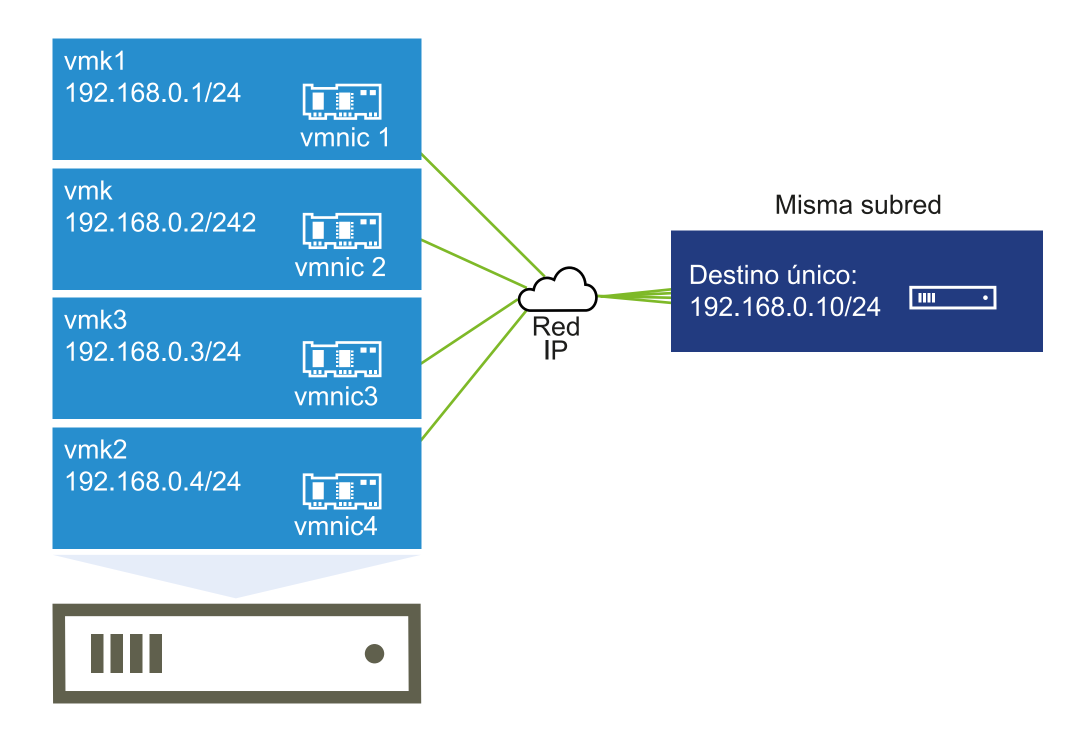
Vea los siguientes ejemplos.

Puertos de VMkernel	Portales de destino	Sesiones iSCSI
2 puertos de VMkernel no enlazados	2 portales de destino	2 sesiones
4 puertos de VMkernel no enlazados	1 portal de destino	1 sesión
2 puertos de VMkernel no enlazados	4 portales de destino	4 sesiones

Creación de múltiples rutas de iSCSI de software

Ejemplo 1. Múltiples rutas para un destino iSCSI con un solo portal de red

Si el destino tiene un solo portal de red, puede crear múltiples rutas para él agregando varios puertos de VMkernel al host ESXi y enlazándolos al iniciador de iSCSI.

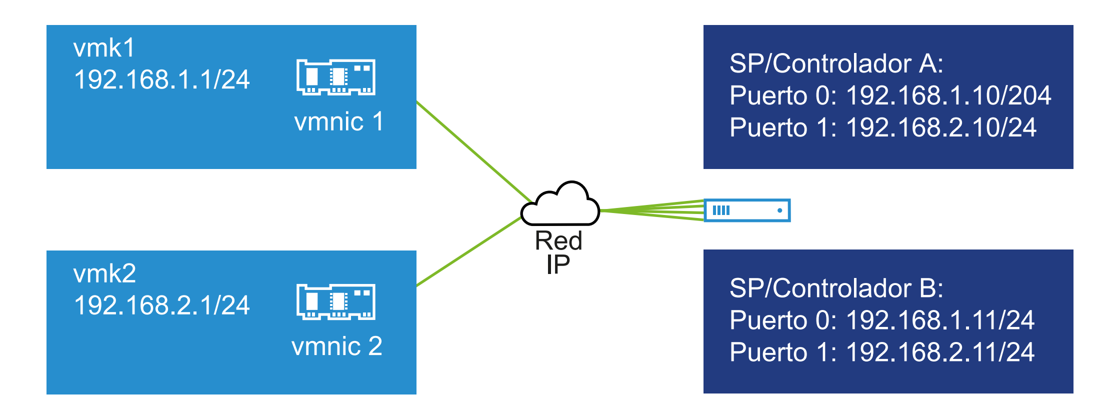


En este ejemplo, todos los puertos de iniciador y el portal de destino están configurados en la misma subred. Es posible acceder al destino mediante todos los puertos enlazados. Cuenta con cuatro puertos de VMkernel y un portal de destino, por lo cual se crea un total de cuatro rutas de acceso.

Sin el enlace de puertos, se crea una sola ruta de acceso.

Ejemplo 2. Múltiples rutas con puertos de VMkernel en diferentes subredes

Puede crear múltiples rutas configurando varios puertos y portales de destino en diferentes subredes IP. Si se mantiene el iniciador y los puertos de destino en diferentes subredes, puede hacer que ESXi cree rutas de acceso mediante puertos específicos. El enlace de puertos no se usa en esta configuración, ya que esto requiere que todos los puertos del iniciador y de destino se encuentren en la misma subred.



ESXi selecciona vmk1 durante la conexión con el puerto 0 del controlador A y controlador B, ya que los tres puertos se encuentran en la misma subred. De modo similar, se selecciona vmk2 durante la conexión con el puerto 1 del controlador A y controlador B. Puede usar la formación de equipos de NIC en esta configuración.

Se crea un total de cuatro rutas de acceso.

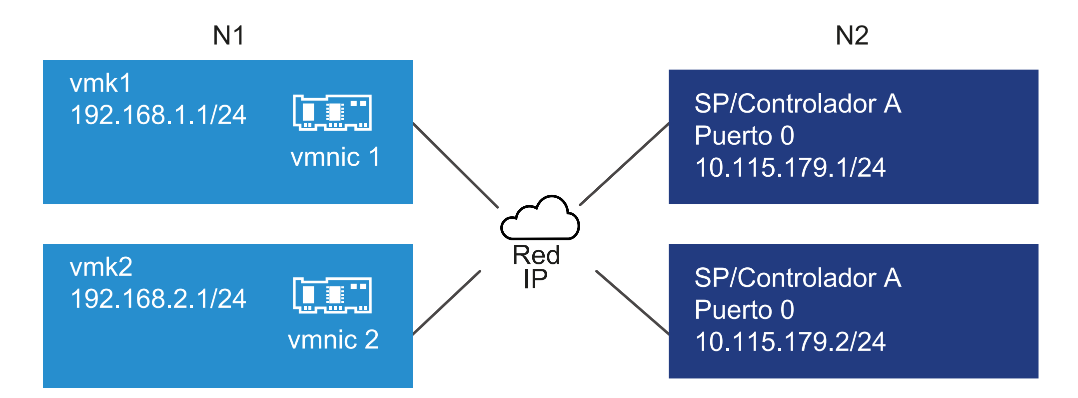
Rutas de acceso	Descripción
Ruta de acceso 1	vmk1 y puerto 0 del controlador A
Ruta de acceso 2	vmk1 y puerto 0 del controlador B
Ruta de acceso 3	vmk2 y puerto 1 del controlador A
Ruta de acceso 4	vmk2 y puerto 1 del controlador B

Enrutamiento con iSCSI de software

Puede usar el comando `esxcli` si desea agregar rutas estáticas para el tráfico de iSCSI. Una vez configuradas las rutas estáticas, los puertos de iniciador y de destino en diferentes subredes pueden comunicarse entre sí.

Ejemplo 1. Uso de rutas estáticas con enlace de puertos

En este ejemplo se conservan todos los puertos de VMkernel enlazados en una subred (N1) y se configuran todos los portales de destino en otra subred (N2). A continuación, se puede agregar una ruta estática para la subred de destino (N2).

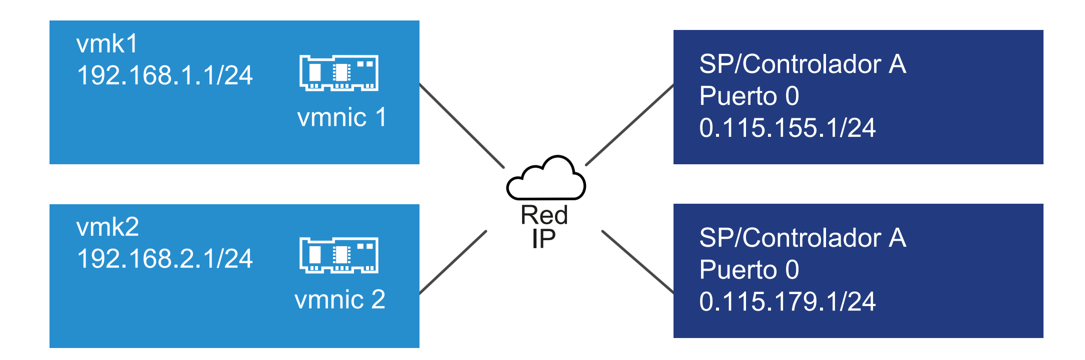


Utilice el siguiente comando:

```
# esxcli network ip route ipv4 add -gateway 192.168.1.253 -network
10.115.179.0/24
```

Ejemplo 2. Uso de rutas estáticas para crear múltiples rutas

En esta configuración, se usan rutas estáticas cuando hay diferentes subredes. No puede usar el enlace de puertos con esta configuración.



Se configuran vmk1 y vmk2 en distintas subredes (192.168.1.0 y 192.168.2.0). Los portales de destino también se encuentran en diferentes subredes (10.115.155.0 y 10.155.179.0).

Puede agregar la ruta estática para 10.115.155.0 desde vmk1. Asegúrese de que pueda accederse a la puerta de enlace desde vmk1.

esxcli network ip route ipv4 add -gateway 192.168.1.253 -network 10.115.155.0/24

A continuación, puede agregar la ruta estática para 10.115.179.0 desde vmk2. Asegúrese de que pueda accederse a la puerta de enlace desde vmk2.

esxcli network ip route ipv4 add -gateway 192.168.2.253 -network 10.115.179.0/24

Durante la conexión con el puerto 0 del controlador A, se usa vmk1.

Durante la conexión con el puerto 0 del controlador B, se usa vmk2.

Ejemplo 3. Enrutamiento con una puerta de enlace distinta por puerto de VMkernel

A partir de vSphere 6.5, se puede configurar una puerta de enlace distinta por cada puerto de VMkernel. Si usa DHCP para obtener la configuración de IP de un puerto de VMkernel, la información de la puerta de enlace también puede obtenerse mediante DHCP.

Para ver la información de la puerta de enlace por cada puerto de VMkernel, utilice el siguiente comando:

esxcli network ip interface ipv4 address list

```
Name  IPv4 Address    IPv4 Netmask   IPv4 Broadcast  Address Type  Gateway         DHCP DNS
----  --------------  -------------  --------------  ------------  --------------  --------
vmk0  10.115.155.122  255.255.252.0  10.115.155.255  DHCP          10.115.155.253      true
vmk1  10.115.179.209  255.255.252.0  10.115.179.255  DHCP          10.115.179.253      true
vmk2  10.115.179.146  255.255.252.0  10.115.179.255  DHCP          10.115.179.253      true
```

Cuando se usan distintas puertas de enlace por cada puerto de VMkernel, el enlace de puertos permite acceder a destinos en diferentes subredes.

Agregar enlaces de puertos en VMware Host Client

Use VMware Host Client para enlazar un adaptador de iSCSI al adaptador de VMkernel del host.

Requisitos previos

- Cree un adaptador VMkernel virtual para cada adaptador de red físico del host. Si utiliza varios adaptadores VMkernel, configure la directiva de red correcta.
- Privilegio necesario:**Host.Configuración.Configuración de partición de almacenamiento**

Procedimiento

1. Haga clic en **Almacenamiento** desde el inventario de VMware Host Client, luego en **Adaptadores** y, por último, en **Configurar iSCSI**.
2. En la sección **Enlaces de puertos de red**, haga clic en **Agregar enlace de puerto**.
3. Seleccione un adaptador VMkernel para unir al adaptador de iSCSI.

   Nota Asegúrese de que la directiva de red del adaptador VMkernel cumpla con los requisitos de unión.

   Se puede vincular el adaptador de iSCSI de software con uno o más adaptadores VMkernel. En el caso de un adaptador de iSCSI de hardware dependiente, solo hay disponible un adaptador VMkernel asociado con la NIC física correcta.
4. Haga clic en **Seleccionar**.
5. Haga clic en **Guardar configuración**.

Quitar enlaces de puertos en VMware Host Client

Para quitar un enlace de puertos, edite la configuración de iSCSI del host.

Procedimiento

1. Haga clic en **Almacenamiento** desde el inventario de VMware Host Client, luego en **Adaptadores** y, por último, en **Configurar iSCSI**.
2. En la sección **Enlaces de puertos de red**, seleccione una NIC de VMkernel de la lista.
3. Haga clic en **Quitar enlace de puertos**.
4. Haga clic en **Guardar configuración**.

Configurar direcciones de detección para adaptadores de iSCSI

Se deben configurar direcciones de detección de destino, para que el adaptador de iSCSI pueda determinar qué recurso de almacenamiento de la red está disponible para el acceso.

El sistema ESXi es compatible con estos métodos de detección:

Detección dinámica

También conocida como detección SendTargets. Cada vez que el iniciador contacta con un servidor iSCSI especificado, el iniciador envía la solicitud de SendTargets al servidor. El servidor responde proporcionando una lista de destinos disponibles al iniciador. Los nombres y las direcciones IP de estos destinos aparecen en la pestaña **Static Discovery** (Detección

estática). Si se quita un destino estático agregado con la detección dinámica, el destino puede ser devuelto a la lista la próxima vez que se vuelva a examinar, que se restablezca el adaptador de iSCSI o que se reinicie el host.

Nota Con iSCSI de hardware dependiente y software, ESXi filtra las direcciones de destino según la familia de IP de la dirección del servidor iSCSI especificado. Si la dirección es IPv4, se filtran las direcciones IPv6 que pueden aparecer en la respuesta SendTargets desde el servidor iSCSI y se las excluye. Cuando se utilizan nombres DNS para especificar un servidor iSCSI o cuando la respuesta SendTargets desde el servidor iSCSI tiene nombres DNS, ESXi depende de la familia de IP de la primera entrada resuelta de la búsqueda de DNS.

Detección estática

Además del método de detección dinámica, se puede utilizar una detección estática e introducir manualmente la información de los destinos. El adaptador de iSCSI utiliza una lista de destinos que se proporcionan para ponerse en contacto y comunicarse con los servidores iSCSI.

Configurar un destino estático en VMware Host Client

Con los iniciadores iSCSI, puede usar la detección estática para introducir manualmente la información de los destinos.

Cuando se configura la detección estática, solo se pueden agregar destinos iSCSI nuevos. No se pueden cambiar la dirección IP, el nombre DNS, el nombre de destino iSCSI ni el número de puerto de un destino existente. Para hacer cambios, quite el destino existente y agregue uno nuevo.

Requisitos previos

Privilegios necesarios: **Host.Configuración.Configuración de partición de almacenamiento**

Procedimiento

1 Haga clic en **Almacenamiento** desde el inventario de VMware Host Client, luego en **Adaptadores** y, por último, en **Configurar iSCSI**.

2 Haga clic en **Agregar destino estático**.

   El nuevo destino estático se muestra en la lista.

3 Si desea agregar un nombre para el nuevo destino estático, haga clic en el destino en la lista y escriba el nombre.

4 Si desea agregar una dirección para el nuevo destino estático, haga clic en el destino en la lista y escriba la dirección.

5 (opcional) Para cambiar el número de puerto del nuevo destino estático, haga clic en el cuadro de texto **Puerto** del destino y escriba el nuevo número de puerto.

6 (opcional) Para editar la configuración del destino estático, seleccione el nuevo destino en la lista de destinos disponibles, haga clic en **Editar configuración**, configure los parámetros que desee modificar y haga clic en **Guardar**.

7 (opcional) Para eliminar un destino específico, seleccione el destino y haga clic en **Eliminar destino estático**.

   El destino ya no aparecerá en la lista de destinos estáticos existentes.

8 Haga clic en **Guardar configuración**.

Configurar un destino dinámico en VMware Host Client

Con la detección dinámica, cada vez que el iniciador se ponga en contacto con un sistema de almacenamiento iSCSI en particular, le enviará una solicitud de SendTargets al sistema iSCSI. El sistema iSCSI le responde al iniciador y le suministra una lista de destinos disponibles.

Cuando se configura la detección dinámica, solo se puede agregar un sistema iSCSI nuevo. No se puede cambiar la dirección IP, el nombre DNS ni el número de puerto del sistema iSCSI existente. Para modificar los parámetros, elimine el sistema existente y agregue uno nuevo.

Requisitos previos

Privilegio necesario: **Host.Configuración.Configuración de partición de almacenamiento**

Procedimiento

1 Haga clic en **Almacenamiento** desde el inventario de VMware Host Client, luego en **Adaptadores** y, por último, en **Configurar iSCSI**.

2 Haga clic en **Agregar destino dinámico**.

   El nuevo destino dinámico se muestra en la lista.

3 Si desea agregar una dirección para el nuevo destino dinámico, haga clic en el destino en la lista y escriba la dirección.

4 (opcional) Para cambiar el número de puerto del nuevo destino dinámico, haga clic en el cuadro de texto **Puerto** del destino y escriba el nuevo número de puerto.

5 (opcional) Para editar la configuración del destino dinámico, seleccione el nuevo destino en la lista de destinos disponibles, haga clic en **Editar configuración**, configure los parámetros que desee modificar y haga clic en **Guardar**.

6 (opcional) Para eliminar un destino específico, seleccione el destino y haga clic en **Eliminar destino dinámico**.

   El destino ya no aparecerá en la lista de destinos dinámicos existentes.

7 Haga clic en **Guardar configuración**.

Editar la configuración avanzada de iSCSI en VMware Host Client

La configuración avanzada de iSCSI controla los parámetros, como el encabezado y el resumen de datos, la redirección de ARP, ACK demorado, etc. Por lo general, no es necesario cambiar esta configuración dado que el host funciona con los valores predefinidos asignados.

Precaución No haga cambios en la configuración de iSCSI avanzada a menos que esté trabajando con el equipo de soporte de VMware o que tenga información detallada sobre los valores que debe asignar al cambio de configuración.

Requisitos previos

Privilegio necesario: **Host.Configuración.Configuración de partición de almacenamiento**

Procedimiento

1 Haga clic en **Almacenamiento** desde el inventario de VMware Host Client, luego en **Adaptadores** y, por último, en **Configurar iSCSI**.

2 Haga clic en **Configuración avanzada** para visualizar la lista completa de ajustes.

3 Edite los parámetros que desea modificar y haga clic en **Guardar configuración**.

Configurar la autenticación CHAP para un adaptador de iSCSI en VMware Host Client

Se pueden configurar todos los destinos de manera que reciban el mismo nombre y secreto de CHAP del iniciador iSCSI en el nivel del iniciador. De forma predeterminada, todas las direcciones de detección o los destinos estáticos heredan los parámetros de CHAP configurados en el nivel del iniciador.

El nombre de CHAP debe tener menos de 511 caracteres alfanuméricos y la contraseña de CHAP menos de 255 caracteres alfanuméricos. Algunos adaptadores, por ejemplo, el adaptador QLogic, pueden tener límites más bajos: 255 caracteres para el nombre de CHAP y 100 para el secreto CHAP.

Requisitos previos

- Antes de configurar los parámetros de CHAP para iSCSI de software o hardware dependiente, indique si desea configurar CHAP unidireccional, también conocido como normal, o CHAP mutuo. Los adaptadores de iSCSI de hardware independiente no admiten CHAP mutuo.
  - En CHAP unidireccional, el destino autentica al iniciador.
  - En CHAP mutuo, el destino y el iniciador se autentican mutuamente. Utilice diferentes contraseñas para CHAP y para CHAP mutuo.

  Al configurar los parámetros de CHAP, compruebe que coincidan con los parámetros del lado del almacenamiento.
- Privilegios necesarios: **Host.Configuración.Configuración de partición de almacenamiento**

Procedimiento

1 Haga clic en **Almacenamiento** desde el inventario de VMware Host Client, luego en **Adaptadores** y, por último, en **Configurar iSCSI**.

2 Para configurar CHAP unidireccional, expanda **Autenticación CHAP** para visualizar todos los parámetros.

   a Seleccione el nivel de seguridad de CHAP.

   b Introduzca el nombre de CHAP.

   Asegúrese de que el nombre que especifique coincida con el nombre configurado en el lado del almacenamiento.

   c Escriba una contraseña de CHAP unidireccional para usar en la autenticación. Utilice la misma contraseña que escribió en el lado del almacenamiento.

3 Para configurar CHAP mutuo, seleccione **Usar CHAP** como opción para CHAP unidireccional. Expanda **Autenticación de CHAP mutuo** para visualizar todos los parámetros.

   a Seleccione **Utilizar CHAP**.

   b Escriba el nombre de CHAP mutuo.

   c Escriba el secreto CHAP mutuo.

   Utilice diferentes contraseñas para CHAP unidireccional y CHAP mutuo.

4 Haga clic en **Guardar configuración**.

Resultados

Si cambia la configuración de autenticación para un adaptador iSCSI, solamente debe usar las credenciales actualizadas para las nuevas sesiones de iSCSI. Las sesiones existentes persisten hasta que la conexión se pierde por algún factor externo, como forzar una reautenticación, o hasta que se quitan y agregan los destinos iSCSI del adaptador.

Administrar dispositivos de almacenamiento en VMware Host Client

Puede usar VMware Host Client para administrar los dispositivos de almacenamiento de red y locales a los que tiene acceso el host ESXi que está administrando.

Ver dispositivos de almacenamiento en VMware Host Client

Vea todos los dispositivos de almacenamiento disponibles para un host. Si se usan complementos de múltiples rutas de terceros, los dispositivos de almacenamiento disponibles por medio de los complementos también aparecen en la lista.

La vista Dispositivos de almacenamiento permite enumerar los dispositivos de almacenamiento de los hosts, analizar su información y modificar sus propiedades.

Procedimiento

1 Haga clic en **Almacenamiento** desde el inventario de VMware Host Client y, a continuación, haga clic en **Dispositivos**.

   Todos los dispositivos de almacenamiento disponibles para el host se enumeran en **Dispositivos**.

2 Para ver los detalles de un dispositivo específico, seleccione el dispositivo en la lista.

Borrar una tabla de particiones de dispositivos en VMware Host Client

Al iniciar sesión en un host ESXi con VMware Host Client, puede borrar la tabla de particiones de un dispositivo de disco que está accesible en el host.

Requisitos previos

Compruebe que ESXi no esté utilizando el dispositivo como disco de arranque, almacén de datos de VMFS o vSAN.

Procedimiento

1 Haga clic en **Almacenamiento** desde VMware Host Client y, a continuación, haga clic en **Dispositivos**.

2 Haga clic con el botón derecho en un dispositivo de la lista, luego en **Borrar tabla de particiones** y, por último, en **Sí**.

   Borrar la tabla de particiones puede producir una pérdida de datos.

Editar particiones de dispositivos individuales en VMware Host Client

Al iniciar sesión en un host ESXi con VMware Host Client, puede quitar particiones individuales de un dispositivo mediante el editor de particiones.

Requisitos previos

Compruebe que ESXi no esté utilizando el dispositivo como disco de arranque, almacén de datos de VMFS o vSAN.

Procedimiento

1 Haga clic en **Almacenamiento** desde VMware Host Client y, a continuación, haga clic en **Dispositivos**.

2 Haga clic con el botón derecho en un dispositivo de la lista y, a continuación, haga clic en **Editar particiones**.

3 Seleccione una partición y haga clic en **Eliminar partición**.

4 (opcional) Haga clic en **Restablecer** para restaurar las particiones originales.

5 Haga clic en **Guardar particiones**.

6 Confirme que desea alterar la partición.

Administrar memoria persistente

ESXi 6.5 es compatible con la tecnología de memoria para equipos más reciente, la cual se conoce como memoria no volátil (Non-Volatile Memory, NVM) o memoria persistente (Persistent Memory, PMem). PMem combina la alta velocidad de transferencia de datos de la memoria volátil del equipo con la persistencia y la resiliencia del almacenamiento tradicional. Los dispositivos de PMem tienen baja latencia de acceso y pueden conservar los datos almacenados tras reinicios o interrupciones de la alimentación.

Modos de uso de los recursos de memoria persistente del host

Al agregar un dispositivo PMem físico a un host, ESXi detecta el recurso de PMem y lo expone como un almacén de datos de PMem de host local a las máquinas virtuales que se ejecutan en el host. En función del sistema operativo invitado, las máquinas virtuales pueden tener acceso directo a los recursos de PMem.

Cada host puede tener un solo almacén de datos PMem local que agrupa y representa todos los recursos de PMem del host.

La memoria persistente combina las propiedades de memoria y almacenamiento. Por lo tanto, las máquinas virtuales pueden consumir los recursos de PMem del host de ESXi como memoria (a través de dispositivos NVDIMM virtuales) o como almacenamiento (a través de discos duros virtuales de PMem).

El almacén de datos de PMem del host local guarda todos los discos duros virtuales de PMem y los dispositivos NVDIMM de acceso directo.

PMem virtual (Virtual PMem, vPMem)

En este modo, si el sistema operativo invitado reconoce PMem, la máquina virtual puede tener acceso directo a los recursos físicos de PMem del host y utilizarlos como memoria direccionable por bytes estándar.

Las máquinas virtuales utilizan módulos de memoria en línea duales no volátiles virtuales (Virtual Non-Volatile Dual In-Line Memory Module, NVDIMM) para acceder a PMem de forma directa. NVDIMM es un dispositivo de memoria que se encuentra en un canal de memoria ordinaria, pero que contiene la memoria no volátil. En vSphere 6.5, NVDIMM virtual es un nuevo tipo de dispositivo que representa las regiones de PMem físicas del host. Una sola máquina virtual puede tener hasta 64 dispositivos virtuales de NVDIMM. Cada dispositivo NVDIMM se almacena en el almacén de datos de PMem local del host.

Nota Para agregar un dispositivo NVDIMM a una máquina virtual, esta debe contar con la versión de hardware 14 y el sistema operativo invitado debe ser compatible con la memoria persistente. Si el sistema operativo invitado no reconoce PMem, puede seguir utilizando PMem, pero no puede agregar un dispositivo NVDIMM a la máquina virtual.

Discos virtuales de PMem (vPMemDisk)

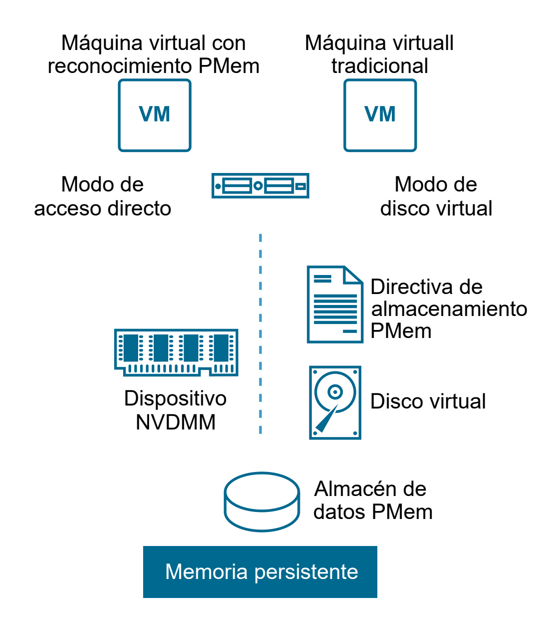
En este modo, la máquina virtual no tiene acceso directo a los recursos de PMem del host.

Debe agregar un disco duro virtual de PMem a la máquina virtual. Un disco duro virtual de PMem es un disco SCSI tradicional al que se aplica la directiva de almacenamiento de PMem. La directiva coloca automáticamente el disco duro en el almacén de datos de PMem local del host.

En este modo de uso, no existen requisitos para la versión de hardware de la máquina virtual y el sistema operativo invitado.

Nota Si el sistema operativo invitado no reconoce PMem, las máquinas virtuales solo pueden utilizar PMem a través de vPMemDisks.

El siguiente diagrama muestra cómo interactúan los componentes de memoria persistente.



Para obtener información acerca de cómo configurar y administrar máquinas virtuales con dispositivos NVDIMM o discos virtuales de memoria persistente, consulte la documentación de *Administrar recursos de vSphere*.

Estructura del almacén de datos PMem

La interfaz de usuario de VMware Host Client proporciona información acerca de la estructura compleja del almacén de datos PMem de host local. Para analizar esta información y utilizarla con fines de solución de problemas y administración, debe estar familiarizado con los conceptos relacionados con esa estructura compleja.

Módulos

En la interfaz de usuario de VMware Host Client, los módulos representan los NVDIMM físicos que están conectados a la placa base del host.

En VMware Host Client, puede comprobar el estado de mantenimiento de cada módulo e identificar los módulos NVDIMM en estado incorrecto.

Conjuntos de intercalación

Los conjuntos de intercalación son grupos lógicos de uno o varios módulos. Estos revelan cómo se distribuye la información entre los DIMM físicos y cómo ESXi lee la información de los módulos. Dado que ESXi lee desde cada conjunto intercalación por turnos, los conjuntos de intercalación garantizan el mejor rendimiento de proceso de memoria.

Por ejemplo, si un conjunto de intercalación consta de dos módulos, ESXi lee la información de los dos DIMM físicos en paralelo y, a continuación, sigue con el siguiente conjunto de intercalación.

La interfaz de usuario de VMware Host Client proporciona información sobre la forma en que los NVDIMM se agrupan en conjuntos de intercalación.

Espacios de nombres

Los espacios de nombres son regiones de intervalos de memoria que se abordan de forma contigua en el NVDIMM. Los espacios de nombres pueden atravesar los conjuntos de intercalación. El almacén de datos PMem se establece además de los espacios de nombres.

En VMware Host Client, puede ver la capacidad, el estado de mantenimiento y el identificador de ubicación de cada espacio de nombres.

Ver información acerca de los módulos, los conjuntos de intercalación y los espacios de nombres en VMware Host Client

En VMware Host Client puede ver información sobre los módulos, los conjuntos entrelazados y los espacios de nombres del almacén de datos de PMem local del host. Como resultado, puede fácilmente identificar un módulo en mal estado y solucionar los problemas.

No puede realizar la mayoría de las tareas tradicionales de administración de almacenes de datos en el almacén de datos de PMem local del host. Sin embargo, puede utilizar la información acerca de los módulos, los conjuntos entrelazados y los espacios de nombres para solución de problemas.

Requisitos previos

Compruebe que el host tenga al menos un dispositivo físico NVDIMM.

Procedimiento

1 En el panel **Navegador**, haga clic en **Almacenamiento**.
2 En la pestaña **Memoria persistente**, vea información sobre el almacén de datos de PMem local del host.
   - Haga clic en **Módulos** para ver información sobre los NVDIMM que conforman el almacén de datos de PMem.

- Haga clic en **Espacios de nombres** para ver información acerca de los espacios de nombres de los NVDIMM.
- Haga clic en **Conjuntos entrelazados** para ver cómo se agrupan los módulos, o NVDIMM físicos, en conjuntos entrelazados.

Eliminar un espacio de nombres en VMware Host Client

En VMware Host Client, puede eliminar los espacios de nombres que no creó ESXi sino un sistema operativo instalado previamente en el equipo host.

Requisitos previos

- Ponga el host en modo de mantenimiento.
- Realice una copia de seguridad del contenido del espacio de nombres si es posible que necesite el contenido en otro momento.

Procedimiento

1. En VMware Host Client, haga clic en **Almacenamiento**.
2. En la pestaña **Memoria persistente**, haga clic en **Espacios de nombres**.
3. (opcional) En la lista de espacios de nombres, compruebe la columna Estado para determinar qué espacios de nombres utiliza actualmente ESXi.

   Para liberar espacio, debe eliminar los espacios de nombres cuyo estado sea En uso.
4. Seleccione un espacio de nombres y haga clic en el icono **Eliminar**.

   Importante Al eliminar un espacio de nombres, se libera espacio en el almacén de datos, pero solo después de reiniciar el host puede utilizar el espacio libre.
5. Haga clic en el icono **Reiniciar host** para reiniciar el host.

Resultados

El espacio de nombres seleccionado se eliminará del almacén de datos PMem. ESXi crea automáticamente un nuevo espacio de nombres que el almacén de datos de PMem puede utilizar. El nuevo espacio de nombres tiene los mismos ID de ubicación, capacidad y tipo que el eliminado.

Supervisar almacenamiento en VMware Host Client

En VMware Host Client, puede supervisar el estado de almacenamiento del host ESXi que está administrando. También puede ver las tareas y los eventos asociados con los distintos almacenes de datos, adaptadores de almacenamiento y dispositivos de almacenamiento en el host que está administrando.

Supervisar almacenes de datos en VMware Host Client

En VMware Host Client, podrá supervisar el estado de un almacén de datos, y los eventos y tareas asociados con él. A partir de vSphere 6.5 Update 1 y después de habilitar el servicio de vSAN en vSphere Client, también puede supervisar el entorno de vSAN.

Procedimiento

1 Haga clic en **Almacenamiento** en el inventario de VMware Host Client.

2 Haga clic en **Almacenes de datos**.

3 Haga clic en un almacén de datos de la lista.

   El almacén de datos se expande en el inventario de VMware Host Client.

4 Haga clic en **Supervisar** debajo el nombre del almacén de datos.

5 (opcional) Haga clic en **Eventos** para ver los eventos asociados con el almacén de datos.

6 (opcional) Haga clic en **vSAN** para ver los parámetros de configuración del entorno de vSAN del host.

7 (opcional) Haga clic en **Hosts** para ver los hosts que se encuentran en este almacén de datos.

8 (opcional) Haga clic en **Estado** para ver los detalles del estado de diversos parámetros, como **Servicio de rendimiento**, **Red**, **Disco físico**, **Datos**, **Clúster** y **Límites**.

Supervisión de vSAN en VMware Host Client

Puede utilizar VMware Host Client para supervisar el entorno de vSAN del host ESXi.

Conceptos de vSAN

VMware vSAN emplea un enfoque definido por software que crea almacenamiento compartido para máquinas virtuales. Virtualiza los recursos locales de almacenamiento físico de hosts ESXi. También los convierte en grupos de almacenamiento que pueden dividirse y asignarse a máquinas virtuales y aplicaciones según sus requisitos de calidad de servicio. vSAN se implementa directamente en el hipervisor ESXi.

Puede configurar vSAN para que funcione como un clúster híbrido o basado íntegramente en tecnología flash. En clústeres híbridos, se utilizan dispositivos flash para la capa de almacenamiento en caché y discos magnéticos para la capa de capacidad de almacenamiento. En los clústeres basados íntegramente en tecnología flash, los dispositivos flash se utilizan para memoria caché y de capacidad.

Puede activar vSAN en sus clústeres de host existentes y cuando cree clústeres nuevos.

Si vSAN se establece en modo automático, vSAN agrega todos los dispositivos locales de capacidad libres a un solo almacén de datos compartido por todos los hosts del clúster de vSAN. vSAN no puede utilizar los dispositivos formateados y que ya contienen cierta información.

Si vSAN se establece en modo manual, vSAN utiliza los dispositivos locales de capacidad que reclamó mediante el uso de vSphere Client. Si no reclamó todos los dispositivos a través de vSphere Client, el tamaño del almacén de datos de vSAN es 0 MB.

Puede expandir el almacén de datos agregando dispositivos de capacidad o hosts con dispositivos de capacidad al clúster. vSAN Funciona mejor cuando todos los hosts ESXi del clúster comparten configuraciones similares o idénticas entre todos los miembros del clúster, lo que incluye configuraciones similares o idénticas para el almacenamiento. Esta configuración coherente equilibra los componentes de almacenamiento de máquinas virtuales en todos los dispositivos y hosts del clúster. Los hosts sin dispositivos locales también pueden participar y ejecutar sus máquinas virtuales en el almacén de datos de vSAN.

Si un host aporta sus dispositivos de almacenamiento local a un almacén de datos de vSAN, debe proporcionar al menos un dispositivo para el almacenamiento en caché flash y al menos un dispositivo para capacidad. Los dispositivos de capacidad también se denominan discos de datos.

Los dispositivos del host que aporta los dispositivos forman un grupo de discos o más. Cada grupo de discos contiene un dispositivo flash de almacenamiento en caché y un dispositivo de capacidad, o varios, para almacenamiento persistente. Cada host puede configurarse para emplear varios grupos de discos.

Para obtener información sobre prácticas recomendadas, consideraciones de capacidad y recomendaciones generales sobre el diseño y el dimensionamiento de un clúster de vSAN, consulte la *Guía de diseño y dimensionamiento de VMware vSAN*.

Características de vSAN

En este tema se resumen las características que se aplican a vSAN, sus clústeres y almacenes de datos.

vSAN ofrece varias ventajas a su entorno.

Tabla 4-1. Características de vSAN

Funciones compatibles	Descripción
Compatibilidad con almacenamiento compartido	vSAN es compatible con funciones de VMware que requieren almacenamiento compartido, como HA, vMotion y DRS. Por ejemplo, si un host está sobrecargado, DRS puede migrar máquinas virtuales a otros hosts del clúster.
Formato en disco	El formato de archivo virtual en disco de vSAN ofrece una administración de instantáneas y clones muy escalable por cada clúster de vSAN. Para obtener información sobre la cantidad de instantáneas y clones de máquinas virtuales que se admite por cada clúster de vSAN, consulte el documento *Valores máximos de configuración*.
Configuraciones híbridas y basadas íntegramente en tecnología flash	vSAN puede configurarse para un clúster híbrido o basado íntegramente en tecnología flash.

Tabla 4-1. Características de vSAN (continuación)

Funciones compatibles	Descripción
Dominios de errores	vSAN admite la configuración de dominios de errores para proteger a los hosts contra errores de los bastidores o los chasis cuando el clúster de vSAN abarca varios bastidores o chasis de servidores blade en un centro de datos.
Servicio del destino iSCSI.	El servicio del destino iSCSI de vSAN permite que los hosts y las cargas de trabajo físicas que se encuentren fuera del clúster de vSAN accedan al almacén de datos de vSAN.
Clúster ampliado	vSAN admite clústeres ampliados que abarcan dos ubicaciones geográficas.
Compatibilidad con clústeres de conmutación por error de Windows Server (Windows Server Failover Clusters, WSFC)	vSAN 6.7 Update 3 y las versiones posteriores admiten las reservas persistentes de SCSI-3 (SCSI-3 Persistent Reservations, SCSI-3 PR) en el nivel de disco virtual que el clúster de conmutación por error de Windows Server (Windows Server Failover Cluster, WSFC) requiere para arbitrar un acceso a un disco compartido entre nodos. La compatibilidad con instancias de SCSI-3 PR permite la configuración de WSFC con un recurso de disco compartido entre las máquinas virtuales de forma nativa en los almacenes de datos de vSAN. Actualmente se admiten las siguientes configuraciones: ■ Hasta 6 nodos de aplicación por clúster. ■ Hasta 64 discos virtuales compartidos por nodo. **Nota** Microsoft SQL Server 2012, o una versión posterior que se ejecute en Microsoft Windows Server 2012 o posterior, calificó para vSAN.
vSAN Health Service	vSAN Health Service incluye pruebas de comprobación de estado configuradas previamente para supervisar, solucionar problemas, diagnosticar causas de problemas de componentes del clúster e identificar riesgos posibles.
Servicio de rendimiento de vSAN	En el servicio de rendimiento de vSAN, se incluyen tablas estadísticas utilizadas para supervisar las E/S por segundo, el rendimiento, la latencia y la congestión. Puede supervisar el rendimiento de un clúster de vSAN, un host, un grupo de discos, un disco y máquinas virtuales.
Integración con las funciones de almacenamiento de vSphere	vSAN se integra con las funciones de administración de datos de vSphere utilizadas tradicionalmente con el almacenamiento VMFS y NFS. Estas funciones incluyen instantáneas, clones vinculados y vSphere Replication.
Directivas de almacenamiento de máquinas virtuales	vSAN funciona con las directivas de almacenamiento de máquina virtual para admitir un enfoque centrado en máquinas virtuales en la administración de almacenamiento. Si no se asigna una directiva de almacenamiento a la máquina virtual durante la implementación, se asigna automáticamente la directiva de almacenamiento predeterminada de vSAN a la máquina virtual.

Tabla 4-1. Características de vSAN (continuación)

Funciones compatibles	Descripción
Aprovisionamiento rápido	vSAN permite el aprovisionamiento rápido de almacenamiento en vCenter Server® durante las operaciones de creación e implementación de máquinas virtuales.
Desduplicación y compresión	vSAN realiza la desduplicación y la compresión a nivel de bloque para ahorrar espacio de almacenamiento. Cuando se habilitan la desduplicación y la compresión en un clúster basado en flash de vSAN, se reducen los datos redundantes dentro de cada grupo de discos. La desduplicación y la compresión son configuraciones para todo el clúster, pero las funciones se aplican a cada grupo de discos de forma individual. Se aplicará vSAN de solo compresión en cada disco.
Cifrado de datos en reposo	vSAN proporciona el cifrado de datos en reposo. Los datos se cifran después de que se llevan a cabo todas las otras operaciones de procesamiento, como la desduplicación. El cifrado de datos en reposo protege los datos de los dispositivos de almacenamiento, en caso de que un dispositivo se quite del clúster.
Compatibilidad con SDK	VMware vSAN SDK for Java es una extensión de VMware vSphere Management SDK. Incluye documentación, bibliotecas y ejemplos de código que ayudan a los desarrolladores a automatizar la instalación, la configuración, la supervisión y la solución de problemas de vSAN.

Supervisión de vSAN en el VMware Host Client

Puede utilizar VMware Host Client para supervisar el entorno de vSAN del host ESXi.

Requisitos previos

El servicio de vSAN debe habilitarse en vSphere Client para poder ver las pantalla relacionadas con vSAN de un almacén de datos.

Procedimiento

1 Haga clic en **Almacenamiento** en el inventario de VMware Host Client.

2 En la pestaña **Almacenes de datos**, haga clic en **Almacén de datos de vSAN**.

   El almacén de datos de vSAN se ampliará en el navegador de VMware Host Client.

3 Haga clic en **Supervisar**.

   En la interfaz de usuario, aparecen las pestañas **vSAN**, **Host** y **Estado**.

Opción	Descripción
vSAN	Muestra las configuraciones del host actual. Puede editar la configuración del modo de recuperación y la desduplicación. También puede ver la configuración de: ■ Cifrado: vSAN admite el cifrado de información del almacén de datos de vSAN completo. ■ Servicio de iSCSI: servicio adicional mediante el servicio de iSCSI. ■ Servicio de rendimiento: recopila datos acerca del funcionamiento del almacén de datos. Por ejemplo, la velocidad de una operación de lectura/escritura.
Hosts	Muestra una lista de todos los hosts del servidor de vSAN con sus direcciones IP y el dominio de errores al que pertenecen.
Estado	La pestaña **Estado** contiene pruebas organizadas por grupos. Estos son los grupos que se muestran: ■ Servicio de rendimiento ■ Red ■ Physical disk (Disco físico) ■ Datos ■ Clúster ■ Límites Cada grupo se etiqueta con un icono de estado de error, advertencia, desconocido o buen estado. El estado del grupo representa el estado más grave de la prueba que pertenece a dicho grupo. Para ver las pruebas y sus descripciones, haga clic en el icono para expandir en la esquina superior derecha del grupo que desee. En el cuadro ampliado, podrá revisar todas las pruebas que pertenezcan al grupo y el resultado de su ejecución, así como obtener más información sobre qué examina cada prueba en el sistema.

4 Seleccione el parámetro de vSAN que desee supervisar.

Editar la configuración de un almacén de datos de vSAN

La configuración de un almacén de datos de vSAN se puede editar cuando tiene que salir de un estado mal configurado del host actual.

En un almacén de datos de vSAN solo se puede editar la configuración de **Modo de notificación** y **Deduplicación**. Estos cambios solo se aplicarán en el host actual. No se sincronizan en los otros hosts que participan en el clúster de vSAN.

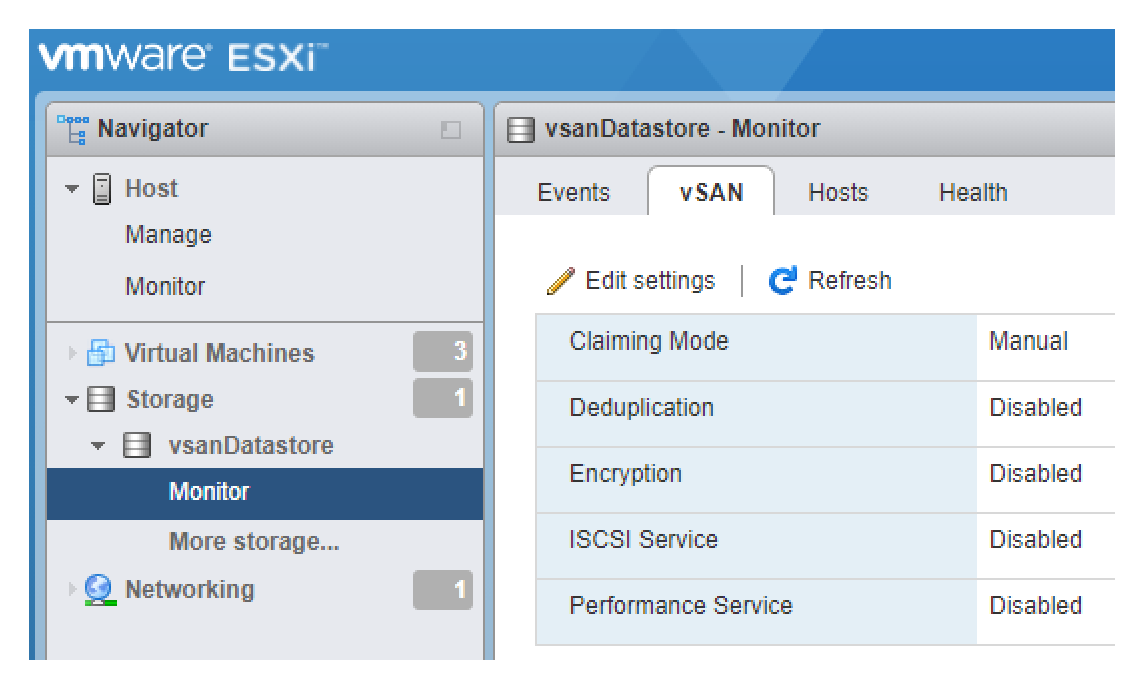
Nota Utilice esta configuración solo para solución de problemas.

Procedimiento

1 Haga clic en **Almacenamiento** en el inventario de VMware Host Client.

2 En la pestaña **Almacenes de datos**, haga clic en un almacén de datos de vSAN de la tabla.

3 Haga clic en **Supervisar** y haga clic en la pestaña **vSAN**.



4 Haga clic en **Editar configuración**.

Se abrirá entonces el cuadro de diálogo **Editar configuración**.

5 Cambie la configuración. Seleccione **Automático** o **Manual** en el **Modo de reclamación**.

Opción	Acción
Modo de reclamación	a Seleccione **Automático** o **Manual** en el **Modo de notificación**. ■ Si selecciona **Automático**, agrupa todos los discos en un grupo o en grupos del mismo tamaño y les envía notificaciones. **Nota** El modo **Automático** está obsoleto. Solo puede notificar a grupos de discos híbridos que no son compatibles con la mayoría de las características de vSAN. ■ Si selecciona **Manual**, debe organizar los discos en grupos y enviarles notificaciones mediante vSphere Web Client manualmente. Por ejemplo, es apropiado seleccionar el modo de notificación manual cuando vCenter Server no está disponible.
Desduplicación	a Seleccione **Habilitado** o **Deshabilitado** para la **Deduplicación**.

6 Haga clic en **Guardar**.

Realizar operaciones para actualizar y volver a examinar almacenamiento en VMware Host Client

La operación de actualización de almacenes de datos, dispositivos de almacenamiento y adaptadores de almacenamiento actualiza la información de almacenamiento y las listas que se muestran en VMware Host Client. Actualiza información como la capacidad de los almacenes

de datos. Cuando realiza tareas de administración de almacenamiento o hace cambios en la configuración de SAN, es posible que necesite volver a examinar el almacenamiento.

Realizar una operación para volver a examinar un adaptador en VMware Host Client

Cuando se hacen cambios en la configuración de SAN y los cambios son exclusivos para el almacenamiento al que se accede a través de un adaptador específico, vuelva a examinar solo ese adaptador. Al volver a examinar un adaptador, detectará todos los LUN nuevos que estén disponibles en el adaptador.

Procedimiento

1 Haga clic en **Almacenamiento** desde el inventario de VMware Host Client y, a continuación, haga clic en **Adaptadores**.
2 Haga clic en **Volver a examinar**.

Volver a examinar un dispositivo en VMware Host Client

Al volver a examinar un dispositivo, detectará todos los volúmenes de VMFS nuevos que estén disponibles en el dispositivo.

Procedimiento

1 Haga clic en **Almacenamiento** desde el inventario de VMware Host Client y, a continuación, haga clic en **Dispositivos**.
2 Haga clic en **Volver a examinar**.

Cambiar la cantidad de dispositivos de almacenamiento examinados en el VMware Host Client

El rango de identificadores de LUN examinados para un host ESXi se encuentra entre 0 y 16.383. ESXi ignora los identificadores de LUN superiores a 16.383. El parámetro `Disk.MaxLUN` configurable controla el rango de identificadores de LUN examinados. El parámetro tiene un valor predeterminado de 1.024.

El parámetro `Disk.MaxLUN` también determina cuántos LUN intentará detectar el código de análisis de SCSI mediante los comandos individuales de consulta INQUIRY si el destino SCSI no admite la detección directa mediante REPORT_LUNS.

Se puede modificar el parámetro `Disk.MaxLUN` según las necesidades. Por ejemplo, si su entorno tiene un número menor de dispositivos de almacenamiento con identificadores de LUN del 1 al 100, establezca el valor en 101. Como resultado, puede mejorar la velocidad de detección de dispositivos en destinos que no admiten REPORT_LUNS. Si se reduce el valor, se puede acortar el tiempo para volver a examinar y el tiempo de arranque. Sin embargo, el tiempo necesario para volver a examinar los dispositivos de almacenamiento también puede depender de otros factores, como el tipo de sistema de almacenamiento y la carga presente en el sistema de almacenamiento.

En otros casos, es posible que haya que aumentar el valor si el entorno utiliza identificadores de LUN mayores que 1023.

Procedimiento

1. Haga clic en **Administrar** desde el inventario de VMware Host Client y, a continuación, haga clic en **Configuración avanzada**.
2. Desplácese hacia abajo hasta `Disk.MaxLUN`.
3. Haga clic con el botón derecho en `Disk.MaxLUN` y después haga clic en **Editar opción**.
4. Escriba un nuevo valor y haga clic en **Guardar**.

   El código de análisis SCSI no analizará los LUN cuyos identificadores sean mayores o iguales que el valor que haya introducido.

   Por ejemplo, para detectar identificadores de LUN del 0 al 100, establezca `Disk.MaxLUN` como 101.

Redes en VMware Host Client

5

Al conectarse a un host ESXi mediante VMware Host Client, puede ver y configurar conmutadores estándares de vSphere. grupos de puertos, NIC físicas, NIC de VMkernel y pilas de TCP/IP.

Este capítulo incluye los siguientes temas:

Administrar grupos de puertos en VMware Host Client

Puede administrar los ajustes de los grupos de puertos para configurar la administración de tráfico y mejorar la seguridad de redes y el rendimiento. Al usar VMware Host Client, puede agregar y eliminar grupos de puertos. También puede examinar la información del grupo de puertos y editar la configuración del grupo de puertos, como la formación de equipos de NIC y la configuración del tráfico.

Ver información del grupo de puertos en VMware Host Client

En VMware Host Client, puede ver información acerca de la configuración de grupos de puertos, los detalles de red, la topología de conmutadores virtuales, la directiva de formación de equipos de NIC, la directiva de descarga y la directiva de seguridad.

Procedimiento

1 Haga clic en **Redes** desde el inventario de VMware Host Client y, a continuación, haga clic en **Grupos de puertos**.

2 Haga clic en un elemento de la lista de grupos de puertos disponibles.

Se muestra información acerca de los detalles de red, la topología de conmutadores virtuales, la directiva de formación de equipos de NIC, la directiva de descarga y la directiva de seguridad.

Agregar un grupo de puertos de conmutador virtual en VMware Host Client

Puede agregar un grupo de puertos a un conmutador virtual en VMware Host Client. Los grupos de puertos ofrecen conexión de red para las máquinas virtuales.

Procedimiento

1 Haga clic con el botón derecho en **Redes** en el inventario de VMware Host Client y, a continuación, haga clic en **Agregar grupo de puertos** en el menú emergente.

2 Introduzca un nombre para el nuevo grupo de puertos.

3 Establezca el identificador de la VLAN para configurar el manejo de la VLAN en el grupo de puertos.

El identificador de VLAN también refleja el modo de etiquetado de VLAN en el grupo de puertos.

Modo de etiquetado de VLAN	Identificador de VLAN	Descripción
Etiquetado de conmutador externo (EST)	0	El conmutador virtual no transmite tráfico asociado con una VLAN.
Etiquetado de conmutador virtual (VST)	De 1 a 4094	El conmutador virtual etiqueta el tráfico con la etiqueta introducida.
Etiquetado de conmutador invitado (VGT)	4095	Las máquinas virtuales controlan las VLAN. El conmutador virtual permite el tráfico desde cualquier VLAN.

4 Seleccione un conmutador virtual en el menú desplegable.

5 Expanda **Seguridad** y seleccione las opciones que quiera habilitar para el modo promiscuo, los cambios de dirección MAC y las transmisiones falsificadas.

6 Haga clic en **Agregar**.

Se crea el grupo de puertos.

7 (opcional) Haga clic en **Actualizar** para mostrar el nuevo grupo de puertos en la lista.

Editar la configuración de grupos de puertos en VMware Host Client

Para mejorar la seguridad de red y su rendimiento en VMware Host Client, puede editar diversos parámetros de configuración del grupo de puertos, como el nombre del grupo de puertos, el identificador de VLAN y el conmutador virtual. También puede configurar los componentes de catalogación de tráfico, formación de equipos de NIC y seguridad.

Procedimiento

1 Haga clic en **Redes** desde el inventario de VMware Host Client y, a continuación, haga clic en **Grupos de puertos**.

2 Haga clic con el botón derecho en el grupo de puertos de la lista que desee editar y seleccione **Editar configuración**.

3 (opcional) Introduzca un nuevo nombre de grupo de puertos.

4 (opcional) Introduzca un nuevo valor para el identificador de VLAN.

   El identificador de VLAN refleja el modo de etiquetado de VLAN en el grupo de puertos.

Modo de etiquetado de VLAN	Identificador de VLAN	Descripción
Etiquetado de conmutador externo (EST)	0	El conmutador virtual no transmite tráfico asociado con una VLAN.
Etiquetado de conmutador virtual (VST)	De 1 a 4094	El conmutador virtual etiqueta el tráfico con la etiqueta introducida.
Etiquetado de conmutador invitado (VGT)	4095	Las máquinas virtuales controlan las VLAN. El conmutador virtual permite el tráfico desde cualquier VLAN.

5 (opcional) Seleccione un conmutador virtual en el menú desplegable.

6 (opcional) Expanda **Seguridad** y seleccione si se deben rechazar, aceptar o heredar las excepciones de la directiva de seguridad desde vSwitch.

Opción	Descripción
Modo promiscuo	■ **Rechazar**. Colocar un adaptador invitado en modo promiscuo no determina qué tramas recibe el adaptador. ■ **Aceptar**. La colocación de un adaptador invitado en modo promiscuo hace que este detecte todos las tramas transmitidas a vSphere Distributed Switch que están permitidas según la directiva de VLAN para el grupo de puertos al que está conectado el adaptador. ■ **Heredar de vSwitch**. La colocación de un adaptador invitado en modo promiscuo provoca que herede la configuración del conmutador virtual asociado.
Cambios de dirección MAC	■ **Rechazar**. Si establece **Cambios de dirección MAC** en **Rechazar** y el sistema operativo invitado cambia la dirección MAC del adaptador por cualquier otra que no sea la especificada en el archivo de configuración `.vmx`, se descartan todas las tramas entrantes. Si el sistema operativo invitado vuelve a cambiar la dirección MAC para que coincida con la dirección MAC del archivo de configuración `.vmx`, se vuelven a pasar las tramas entrantes. ■ **Aceptar**. Al cambiar la dirección MAC del sistema operativo invitado se obtiene el efecto pretendido: se reciben las tramas hacia la nueva dirección MAC. ■ **Heredar de vSwitch**. Si establece **Cambios de dirección MAC** en **Heredar de vSwitch**, la dirección MAC cambia a uno de los conmutadores virtuales asociados.
Transmisiones falsificadas	■ **Rechazar**. Se descartará toda trama saliente con una dirección MAC de origen que sea diferente de la establecida en el adaptador. ■ **Aceptar**. No se realizará ningún filtrado y se pasarán todas las tramas salientes. ■ **Heredar de vSwitch**. La configuración de trama saliente se hereda del conmutador virtual asociado.

7 (opcional) Expanda **Formación de equipos de NIC** y configure los siguientes componentes.

Opción	Descripción
Equilibrio de carga	Especifique de qué forma elegir un vínculo superior. ■ **Heredar de vSwitch**. Elija el vínculo superior que está seleccionado para el conmutador virtual asociado. ■ **Enrutar según el hash de IP**. Elija un vínculo superior basado en un hash de las direcciones IP de origen y de destino de cada paquete. Para los paquetes que no utilizan IP, lo que se encuentre en estos desplazamientos se utiliza para calcular el hash. ■ **Enrutar según el hash de MAC de origen**. Elija un vínculo superior basado en un hash de la Ethernet de origen. ■ **Enrutar según el identificador de puerto de origen**. Elija el vínculo superior según el identificador de puerto de origen. ■ **Utilizar orden explícito de conmutación por error**. Utilice siempre el vínculo superior de orden más elevado de la lista de adaptadores activos, que cumpla los criterios de detección de conmutación por error. **Nota** La formación de equipos basada en IP requiere que el conmutador físico se configure con EtherChannel. Se debe deshabilitar EtherChannel para todas las demás opciones.
Detección de conmutación por error de red	Especifique el método que se utilizará para la detección de conmutación por error. ■ ■ **Heredar de vSwitch**. Hereda la configuración correspondiente del conmutador virtual asociado. ■ **Solo estado de vínculo**. Se basa solamente en el estado del vínculo que proporciona el adaptador de red. Esta opción detecta errores, como cables extraídos y errores de alimentación de conmutadores físicos, pero no errores de configuración, como puertos de conmutadores físicos bloqueados por árboles de expansión o configurados hacia la VLAN incorrecta, o cables extraídos en el otro extremo de un conmutador físico. ■ **Solo señal**. Envía y escucha sondas de señal en todas las NIC del equipo, y utiliza esta información, además del estado del vínculo, para determinar el error en el vínculo. Se detectan muchos de los errores que no pueden detectarse solo con el estado del vínculo. **Nota** No utilice sondeo de señal con equilibrio de carga de hash de IP.

Opción	Descripción
Notificar a conmutadores	Seleccione **Sí**, **No** o **Heredar de vSwitch** para notificar a los conmutadores si se produce una conmutación por error. Si selecciona **Sí**, cuando una NIC virtual esté conectada al conmutador distribuido o el tráfico de la NIC virtual se enrute a través de una NIC física diferente en el equipo debido a un evento de conmutación por error, se envía una notificación por la red para actualizar las tablas de búsqueda en los conmutadores físicos. En casi todos los casos, este proceso se recomienda para la latencia más baja de casos de conmutación por error y migración con vMotion. **Nota** No utilice esta opción cuando las máquinas virtuales que utilizan el grupo de puertos estén utilizando el equilibrio de carga de red de Microsoft en modo de unidifusión. Este problema no existe cuando se ejecuta NLB en modo de multidifusión.
Conmutación por recuperación	Seleccione **Sí**, **No** o **Heredar de vSwitch** para deshabilitar o habilitar la conmutación por recuperación. Esta opción determina de qué forma un adaptador físico vuelve a activarse después de recuperarse de un error. Si la conmutación por recuperación se establece en **Sí**, el adaptador vuelve a servicio activo inmediatamente después de recuperarse, y desplaza así a cualquier adaptador en espera que hubiera ocupado su ranura, si lo hubiere. Si la conmutación por recuperación se establece en **No**, un adaptador con errores se deja inactivo incluso después de la recuperación hasta que otro adaptador actualmente activo presente errores y requiera su sustitución.
Orden de conmutación por error	Especifique de qué forma se distribuye la carga de trabajo en los vínculos superiores. Si desea utilizar algunos vínculos superiores, pero reservar otros para emergencias en caso de que los vínculos superiores en uso presenten errores, establezca esta condición moviéndolos a diferentes grupos: ■ **Vínculos superiores activos**. Siga utilizando el vínculo superior si la conectividad del adaptador de red está activa y en funcionamiento. ■ **Vínculos superiores en espera**. Utilice este vínculo superior si la conectividad de uno de los adaptadores activos está desactivada. **Nota** Cuando se utilice el equilibrio de carga de hash de IP, no configure vínculos superiores en espera. No puede configurar el orden de conmutación por error si ninguno de los componentes de grupo de puertos está configurado para heredar la configuración del conmutador virtual asociado.

8 (opcional) Para configurar la catalogación de tráfico, expanda **Catalogación de tráfico**, haga clic en **Habilitada** y especifique los siguientes parámetros.

Opción	Descripción
Ancho de banda promedio	Establece la cantidad de bits por segundo para limitar en un puerto, con un promedio a lo largo del tiempo (carga promedio permitida).
Ancho de banda máximo	La cantidad máxima de bits por segundo para limitar en un puerto cuando se envía o recibe una ráfaga de tráfico. Este es el ancho de banda máximo utilizado por un puerto cada vez que este utilice las ráfagas adicionales.
Tamaño de ráfaga	Es la cantidad máxima de bytes para limitar en una ráfaga. Si se establece este parámetro, un puerto podría recibir una ráfaga adicional cuando no utiliza todo el ancho de banda asignado. Cada vez que el puerto necesita más ancho de banda que el especificado por el parámetro **Ancho de banda promedio**, se le puede permitir que transmita datos de forma temporal a una velocidad más alta, si hay disponible una ráfaga adicional. Este parámetro representa la cantidad de bytes máxima que pueden acumularse en la ráfaga adicional y transferirse a una velocidad más alta.

La directiva de catalogación de tráfico se aplica al tráfico de cada adaptador de red virtual conectado al conmutador virtual.

9 Haga clic en **Guardar** para aplicar los cambios.

Quitar un grupo de puertos de conmutadores virtuales en VMware Host Client

Puede quitar grupos de puertos de los conmutadores virtuales si ya no necesita las redes etiquetadas asociadas.

Requisitos previos

Compruebe que no existan NIC de VMkernel ni máquinas virtuales encendidas conectadas al grupo de puertos que desea quitar.

Procedimiento

1 Haga clic en **Redes** en el inventario de VMware Host Client y, a continuación, haga clic en la pestaña **Grupos de puertos**.

2 Haga clic con el botón derecho en el grupo de puertos que desee quitar y seleccione **Quitar** en el menú emergente.

3 Para quitar el grupo de puertos, haga clic en **Quitar**.

4 (opcional) Haga clic en **Actualizar** para verificar que haya quitado el grupo de puertos.

Administrar conmutadores virtuales en VMware Host Client

En VMware Host Client, puede configurar diversos parámetros del conmutador virtual, como detección de vínculos, formación de equipos de NIC y catalogación de tráfico.

Ver información de conmutadores virtuales en VMware Host Client

En VMware Host Client, puede ver información acerca de conmutadores virtuales, como la configuración, los detalles de red, la topología de los conmutadores virtuales, etc.

Procedimiento

1 Haga clic en **Redes** desde el inventario de VMware Host Client y, a continuación, haga clic en **Conmutadores virtuales**.

2 Haga clic en un conmutador de la lista de conmutadores virtuales disponibles.

   Se muestra información acerca de la configuración de conmutadores virtuales, los detalles de red y la topología de los conmutadores virtuales.

Agregar un conmutador virtual estándar en VMware Host Client

En VMware Host Client, puede agregar un conmutador virtual estándar para proporcionar conectividad de red para el host que está administrando y para las máquinas virtuales que residen en ese host, y también para manejar el tráfico de VMkernel. Según el tipo de conexión que desee crear, puede crear un conmutador estándar de vSphere con un adaptador de VMkernel, conectar un adaptador de red físico existente al nuevo conmutador o crear el conmutador con un grupo de puertos de máquina virtual.

Procedimiento

1 Haga clic con el botón derecho en **Redes** en el inventario de VMware Host Client y, a continuación, haga clic en **Agregar vSwitch estándar** en el menú desplegable.

2 (opcional) Haga clic en **Agregar vínculo superior** para agregar un nuevo vínculo superior físico a un conmutador virtual.

3 Introduzca un nombre para el conmutador virtual y haga clic en **Crear conmutador virtual**.

4 Seleccione una vínculo superior para el conmutador virtual.

5 Expanda **Detección de vínculos** y seleccione una opción para el modo de conmutador virtual.

Operación	Descripción
Escuchar	ESXi detecta y muestra la información sobre el puerto de conmutador físico asociado, pero no permite que el administrador de conmutadores vea la información sobre el conmutador estándar de vSphere.
Anunciar	ESXi permite que el administrador de conmutadores vea la información sobre el conmutador estándar de vSphere, pero no detecta ni muestra información sobre el conmutador físico.
Ambas	ESXi detecta y muestra información sobre el conmutador físico asociado y permite que el administrador de conmutadores vea la información sobre el conmutador estándar de vSphere.
Ninguna	ESXi no detecta ni muestra la información sobre el puerto de conmutador físico asociado, y tampoco permite que el administrador de conmutadores vea la información sobre el conmutador estándar de vSphere.

6 En la sección Protocolo, seleccione **Cisco Discovery Protocol** en el menú desplegable.

7 Expanda **Seguridad** y acepte o rechace el modo promiscuo, los cambios de dirección MAC y las transmisiones falsificadas de las máquinas virtuales adjuntas al conmutador estándar.

Opción	Descripción
Modo promiscuo	■ **Rechazar**. El adaptador de red de máquina virtual recibe únicamente tramas dirigidas a la máquina virtual. ■ **Aceptar**. El conmutador virtual envía todas las tramas a la máquina virtual de acuerdo con la directiva de VLAN vigente para el puerto en el cual está conectado el adaptador de red de máquina virtual. **Nota** El modo promiscuo no es un modo seguro de funcionamiento. Los firewall, los escáneres de puertos y los sistemas de detección de intrusiones deben ejecutarse en modo promiscuo.
Cambios de dirección MAC	■ **Rechazar**. Si el sistema operativo invitado cambia la dirección MAC efectiva de la máquina virtual a un valor diferente de la dirección MAC del adaptador de red de máquina virtual (establecido en el archivo de configuración de `.vmx`), el conmutador descarta todas las tramas entrantes al adaptador. Si el sistema operativo invitado vuelve a cambiar la dirección MAC efectiva de la máquina virtual a la dirección MAC del adaptador de red de máquina virtual, la máquina virtual recibe las tramas nuevamente. ■ **Aceptar**. Si el sistema operativo invitado cambia la dirección MAC efectiva de la máquina virtual a un valor distinto de la dirección MAC del adaptador de red de máquina virtual, el conmutador permite que pasen las tramas a la dirección nueva.
Transmisiones falsificadas	■ **Rechazar**. el conmutador descarta cualquier trama saliente desde el adaptador de máquina virtual con una dirección MAC de origen que sea diferente de la que aparece en el archivo de configuración `.vmx`. ■ **Aceptar**. El conmutador no filtra y acepta todas las tramas salientes.

8 Haga clic en **Agregar**.

Quitar un conmutador virtual estándar en VMware Host Client

Puede quitar el conmutador virtual estándar en caso de que ya no lo necesite.

Procedimiento

1 Haga clic en **Redes** en el inventario de VMware Host Client y, a continuación, haga clic en la pestaña **Conmutadores virtuales**.

2 Haga clic en el botón derecho en el conmutador virtual que desee quitar de la lista y, a continuación, haga clic en **Quitar**.

3 Haga clic en **Sí**.

Agregar un vínculo superior físico en un conmutador virtual en VMware Host Client

Se pueden conectar varios adaptadores a un único conmutador estándar de vSphere para generar la formación de equipos de NIC. El equipo puede compartir tráfico y proporcionar conmutación por error.

Procedimiento

1 Haga clic en **Redes** desde el inventario de VMware Host Client y, a continuación, haga clic en **Conmutadores virtuales**.

2 Haga clic en una máquina virtual de la lista y, a continuación, en **Agregar vínculo superior**.

3 Seleccione una NIC física de las opciones disponibles.

4 Haga clic en **Guardar**.

Editar la configuración de conmutadores virtuales en VMware Host Client

En VMware Host Client, puede editar la configuración de los conmutadores virtuales, como los vínculos superiores de conmutador virtual.

Procedimiento

1 Haga clic en **Redes** desde el inventario de VMware Host Client y, a continuación, haga clic en **Conmutadores virtuales**.

2 Haga clic con el botón secundario en el conmutador virtual que desee editar y, a continuación, en **Editar configuración**.

3 (opcional) Haga clic en **Agregar vínculo superior** para agregar un nuevo vínculo superior físico al conmutador virtual.

4 Cambie la unidad de transmisión máxima (MTU).

   La MTU mejora la eficiencia de red aumentando la cantidad de datos de la carga útil transmitidos con un solo paquete, es decir, que habilita tramas gigantes.

5 (opcional) Haga clic en el icono **Quitar** (⊗) para quitar el vínculo superior anterior del conmutador virtual.

6 Expanda **Detección de vínculos** y seleccione una opción para el modo de conmutador virtual.

Operación	Descripción
Escuchar	ESXi detecta y muestra la información sobre el puerto de conmutador físico asociado, pero no permite que el administrador de conmutadores vea la información sobre el conmutador estándar de vSphere.
Anunciar	ESXi permite que el administrador de conmutadores vea la información sobre el conmutador estándar de vSphere, pero no detecta ni muestra información sobre el conmutador físico.

Operación	Descripción
Ambas	ESXi detecta y muestra información sobre el conmutador físico asociado y permite que el administrador de conmutadores vea la información sobre el conmutador estándar de vSphere.
Ninguna	ESXi no detecta ni muestra la información sobre el puerto de conmutador físico asociado, y tampoco permite que el administrador de conmutadores vea la información sobre el conmutador estándar de vSphere.

7 En la sección Protocolo, seleccione **Cisco Discovery Protocol** en el menú desplegable.

8 Expanda **Seguridad** y acepte o rechace el modo promiscuo, los cambios de dirección MAC y las transmisiones falsificadas de las máquinas virtuales adjuntas al conmutador estándar.

Opción	Descripción
Modo promiscuo	■ **Rechazar**. El adaptador de red de máquina virtual recibe únicamente tramas dirigidas a la máquina virtual. ■ **Aceptar**. El conmutador virtual envía todas las tramas a la máquina virtual de acuerdo con la directiva de VLAN vigente para el puerto en el cual está conectado el adaptador de red de máquina virtual. **Nota** El modo promiscuo no es un modo seguro de funcionamiento. Los firewall, los escáneres de puertos y los sistemas de detección de intrusiones deben ejecutarse en modo promiscuo.
Cambios de dirección MAC	■ **Rechazar**. Si el sistema operativo invitado cambia la dirección MAC efectiva de la máquina virtual a un valor diferente de la dirección MAC del adaptador de red de máquina virtual (establecido en el archivo de configuración de `.vmx`), el conmutador descarta todas las tramas entrantes al adaptador. Si el sistema operativo invitado vuelve a cambiar la dirección MAC efectiva de la máquina virtual a la dirección MAC del adaptador de red de máquina virtual, la máquina virtual recibe las tramas nuevamente. ■ **Aceptar**. Si el sistema operativo invitado cambia la dirección MAC efectiva de la máquina virtual a un valor distinto de la dirección MAC del adaptador de red de máquina virtual, el conmutador permite que pasen las tramas a la dirección nueva.
Transmisiones falsificadas	■ **Rechazar**. el conmutador descarta cualquier trama saliente desde el adaptador de máquina virtual con una dirección MAC de origen que sea diferente de la que aparece en el archivo de configuración `.vmx`. ■ **Aceptar**. El conmutador no filtra y acepta todas las tramas salientes.

9 (opcional) Expanda **Formación de equipos de NIC** y configure los siguientes componentes.

Opción	Descripción
Equilibrio de carga	Especifique de qué forma elegir un vínculo superior. ■ **Enrutar según el hash de IP**. Elija un vínculo superior basado en un hash de las direcciones IP de origen y de destino de cada paquete. Para los paquetes que no utilizan IP, lo que se encuentre en estos desplazamientos se utiliza para calcular el hash. ■ **Enrutar según el hash de MAC de origen**. Elija un vínculo superior basado en un hash de la Ethernet de origen. ■ **Enrutar según el identificador de puerto de origen**. Elija el vínculo superior según el identificador de puerto de origen. ■ **Utilizar orden explícito de conmutación por error**. Utilice siempre el vínculo superior de orden más elevado de la lista de adaptadores activos, que cumpla los criterios de detección de conmutación por error. **Nota** La formación de equipos basada en IP requiere que el conmutador físico se configure con EtherChannel. Se debe deshabilitar EtherChannel para todas las demás opciones.
Detección de conmutación por error de red	Especifique el método que se utilizará para la detección de conmutación por error. ■ **Solo estado de vínculo**. Se basa solamente en el estado del vínculo que proporciona el adaptador de red. Esta opción detecta errores, como cables extraídos y errores de alimentación de conmutadores físicos, pero no errores de configuración, como puertos de conmutadores físicos bloqueados por árboles de expansión o configurados hacia la VLAN incorrecta, o cables extraídos en el otro extremo de un conmutador físico. ■ **Solo señal**. Envía y escucha sondas de señal en todas las NIC del equipo, y utiliza esta información, además del estado del vínculo, para determinar el error en el vínculo. Se detectan muchos de los errores mencionados anteriormente que no pueden detectarse solo con el estado del vínculo. **Nota** No utilice sondeo de señal con equilibrio de carga de hash de IP.
Notificar a conmutadores	Seleccione **Sí**, **No** o **Heredar de vSwitch** para notificar a los conmutadores en caso de error. Si selecciona **Sí**, siempre que haya una NIC virtual conectada al conmutador distribuido o siempre que el tráfico de la NIC virtual se enrute por otra NIC física en el equipo debido a un evento de conmutación por error, se envía una notificación a la red para actualizar las tablas de búsqueda en los conmutadores físicos. En casi todos los casos, este proceso se recomienda para la latencia más baja de casos de conmutación por error y migración con vMotion. **Nota** No utilice esta opción cuando las máquinas virtuales que utilizan el grupo de puertos estén utilizando el equilibrio de carga de red de Microsoft en modo de unidifusión. Este problema no existe cuando se ejecuta NLB en modo de multidifusión.

Opción	Descripción
Conmutación por recuperación	Seleccione **Sí**, **No** o **Heredar de vSwitch** para deshabilitar o habilitar la conmutación por recuperación. Esta opción determina de qué forma un adaptador físico vuelve a activarse después de recuperarse de un error. Si la conmutación por recuperación se establece en **Yes** (Sí) —predeterminado—, el adaptador vuelve a servicio activo inmediatamente después de recuperarse, desplazando a cualquier adaptador en espera que hubiera ocupado su ranura. Si la conmutación por recuperación se establece en **No**, un adaptador con errores se deja inactivo incluso después de la recuperación hasta que otro adaptador actualmente activo presente errores y requiera su sustitución.
Orden de conmutación por error	Especifique de qué forma se distribuye la carga de trabajo en los vínculos superiores. Si desea utilizar algunos vínculos superiores, pero reservar otros para emergencias en caso de que los vínculos superiores en uso presenten errores, establezca esta condición moviéndolos a diferentes grupos: ■ **Vínculos superiores activos**. Siga utilizando el vínculo superior si la conectividad del adaptador de red está activa y en funcionamiento. ■ **Vínculos superiores en espera**. Utilice este vínculo superior si la conectividad de uno de los adaptadores activos está desactivada. **Nota** Cuando se utilice el equilibrio de carga de hash de IP, no configure vínculos superiores en espera.

10 (opcional) Para configurar la catalogación de tráfico, expanda **Catalogación de tráfico**, haga clic en **Habilitada** y especifique los siguientes parámetros.

Opción	Descripción
Ancho de banda promedio	Establece la cantidad de bits por segundo que se permite en un puerto, con un promedio a lo largo del tiempo (carga promedio permitida).
Ancho de banda máximo	Es la cantidad máxima de bits por segundo que se permite en un puerto cuando este envía o recibe una ráfaga de tráfico. Esta cantidad máxima supera el ancho de banda utilizado por un puerto cada vez que este utilice las ráfagas adicionales.
Tamaño de ráfaga	Es la cantidad máxima de bytes que se permiten en una ráfaga. Si se establece este parámetro, un puerto podría obtener una ráfaga adicional si no utiliza todo su ancho de banda asignado. Cuando el puerto necesita más ancho de banda que el especificado por la opción **Ancho de banda promedio**, se le puede permitir la transmisión temporal de datos a una mayor velocidad si hay una ráfaga adicional disponible. Este parámetro establece la cantidad máxima de bytes que se pueden acumular en la ráfaga adicional y se pueden transferir a una velocidad mayor.

La directiva de catalogación de tráfico se aplica al tráfico de cada adaptador de red virtual conectado al conmutador virtual.

11 Haga clic en **Guardar**.

Administrar adaptadores de red físicos en VMware Host Client

Asigne un adaptador físico a un conmutador estándar para brindar conectividad a las máquinas virtuales y los adaptadores VMkernel del host que está administrando.

Ver información de adaptadores de red físicos en VMware Host Client

En VMware Host Client, puede ver información diversa acerca de la configuración y las opciones de los adaptadores de red físicos (NIC).

Procedimiento

1 Haga clic en **Redes** desde el inventario de VMware Host Client y, a continuación, haga clic en **NIC físicas**.

2 Haga clic en el adaptador de red para el cual desee ver información.

Editar NIC físicas en VMware Host Client

Puede editar la velocidad de las NIC físicas mediante VMware Host Client.

Procedimiento

1 Haga clic en **Redes** desde el inventario de VMware Host Client y, a continuación, haga clic en **NIC físicas**.

2 Seleccione la NIC en la tabla que desee editar.

3 Haga clic en **Editar configuración** y seleccione la velocidad en el menú desplegable.

4 Haga clic en **Guardar**.

Administrar adaptadores de red de VMkernel en VMware Host Client

En VMware Host Client, puede agregar y quitar adaptadores de red de VMkernel (NIC), además de ver y modificar la configuración de NIC de VMkernel.

Ver información de adaptadores de red de VMkernel en VMware Host Client

En VMware Host Client, puede ver información acerca de adaptadores de red de VMkernel (NIC), como la configuración de TCP/IP, los detalles de red, la topología de los conmutadores virtuales, etc.

Procedimiento

1 Haga clic en **Redes** desde el inventario de VMware Host Client y, a continuación, haga clic en **NIC de VMkernel**.

2 Haga clic en una NIC de la lista para ver detalles de la configuración y la topología.

Agregar un adaptador de red de VMkernel en VMware Host Client

Es posible agregar un adaptador de red (NIC) de VMkernel a un conmutador de VMware vSphere® Standard Edition™ para proporcionar conectividad de red para los hosts. Además, la NIC de VMkernel controla el tráfico del sistema para VMware vSphere® vMotion®, almacenamiento IP, Fault Tolerance, registro y vSAN, entre otros.

Procedimiento

1 Haga clic con el botón derecho en **Redes** desde el inventario de VMware Host Client y, a continuación, haga clic en **Agregar NIC de VMkernel**.

2 En el cuadro de diálogo **Agregar NIC de VMkernel**, configure los ajustes para el adaptador de VMkernel.

Opción	Descripción
Etiqueta Nuevo grupo de puertos	Al agregar una NIC de VMkernel, también se agrega un grupo de puertos. Especifique un nombre para ese grupo de puertos.
identificador de VLAN	Introduzca un identificador de VLAN a fin de determinar la VLAN que se utilizará para el tráfico de red del adaptador de VMkernel.
Versión de IP	Seleccione IPv4, IPv6 o ambas. **Nota** La opción IPv6 no aparece en los hosts en los que no se ha habilitado IPv6.

3 Seleccione un conmutador virtual en el menú desplegable.

4 (opcional) Expanda la sección de configuración de IPv4 y seleccione una opción para obtener las direcciones IP.

Opción	Descripción
Use DHCP para obtener la configuración de IP.	La configuración de IP se obtiene automáticamente. Debe haber un servidor DHCP presente en la red.
Usar configuración de IP estática	Introduzca la dirección IPv4 y la máscara de subred para el adaptador de VMkernel. Las direcciones de servidor DNS y puerta de enlace predeterminada de VMkernel para IPv4 se obtienen de la pila TCP/IP seleccionada.

5 (opcional) Expanda la sección de configuración de IPv6 y seleccione una opción para obtener las direcciones IPv6.

Opción	Descripción
DHCPv6	Use DHCP para obtener las direcciones IPv6. Debe haber un servidor DHCPv6 presente en la red.
Configuración automática	Use el anuncio de enrutador para obtener las direcciones IPv6.
Direcciones IPv6 estáticas	a Haga clic en **Agregar dirección** para agregar una nueva dirección IPv6. b Introduzca la dirección IPv6 y la longitud del prefijo de subred.

6 Seleccione una pila de TCP/IP en el menú desplegable.

Después de establecer una pila de TCP/IP para el adaptador de VMkernel, no es posible cambiarla posteriormente. Si selecciona vMotion o la pila de TCP/IP de aprovisionamiento, podrá utilizar solamente esta pila para controlar vMotion o el tráfico de aprovisionamiento en el host. Todos los adaptadores de VMkernel para vMotion en la pila de TCP/IP predeterminada se deshabilitan para las sesiones futuras de vMotion. Si utiliza la pila de TCP/IP de aprovisionamiento, los adaptadores de VMkernel de la pila de TCP/IP predeterminada se deshabilitan y no puede realizar algunas operaciones. Estas operaciones incluyen el tráfico de aprovisionamiento, como la migración en frío, la clonación y la migración de instantáneas de máquinas virtuales.

7 (opcional) Seleccione los servicios que desea habilitar para la pila de TCP/IP predeterminada en el host.

vMotion permite al adaptador de VMkernel anunciarse a otro host como la conexión de red mediante la cual se envía el tráfico de vMotion. No puede usar vMotion para realizar migraciones a hosts seleccionados si el servicio de vMotion no está habilitado para ningún adaptador de VMkernel en la pila de TCP/IP predeterminada, o si ningún adaptador usa la pila de TCP/IP de vMotion.

8 Revise sus selecciones de configuración y haga clic en **Crear**.

Editar la configuración de adaptador de red de VMkernel en VMware Host Client

Puede ser necesario modificar el tipo de tráfico admitido para un adaptador de red de VMkernel o la forma en que se obtienen las direcciones IPv4 o IPv6.

Procedimiento

1 Haga clic en **Redes** desde el inventario de VMware Host Client y, a continuación, haga clic en **NIC de VMkernel**.

2 Seleccione el adaptador de VMkernel que reside en el conmutador estándar de destino, haga clic en **Acciones** y seleccione **Editar configuración** en el menú desplegable.

3 (opcional) Edite el identificador de VLAN.

El identificador de VLAN determina la VLAN que se utilizará para el tráfico de red del adaptador de VMkernel.

4 (opcional) Para editar la versión de IP, seleccione IPv4, IPv6 o ambas opciones en el menú desplegable.

Nota La opción IPv6 no aparece en los hosts en los que no se ha habilitado IPv6.

5 (opcional) Expanda la sección de configuración de IPv4 y seleccione una opción para obtener las direcciones IP.

Opción	Descripción
Use DHCP para obtener la configuración de IP.	La configuración de IP se obtiene automáticamente. Debe haber un servidor DHCP presente en la red.
Usar configuración de IP estática	Introduzca la dirección IPv4 y la máscara de subred para el adaptador de VMkernel. Las direcciones de servidor DNS y puerta de enlace predeterminada de VMkernel para IPv4 se obtienen de la pila TCP/IP seleccionada.

6 (opcional) Expanda la sección de configuración de IPv6 y seleccione una opción para obtener las direcciones IPv6.

Opción	Descripción
DHCPv6	Use DHCP para obtener las direcciones IPv6. Debe haber un servidor DHCPv6 presente en la red.
Configuración automática	Use el anuncio de enrutador para obtener las direcciones IPv6.
Direcciones IPv6 estáticas	a Haga clic en **Agregar dirección** para agregar una dirección IPv6. b Introduzca la dirección IPv6 y la longitud del prefijo de subred.

7 (opcional) Seleccione el servicio que desea habilitar o deshabilitar para la pila de TCP/IP predeterminada en el host.

vMotion permite al adaptador de VMkernel anunciarse a otro host como la conexión de red mediante la cual se envía el tráfico de vMotion. No es posible usar vMotion para realizar migraciones a hosts seleccionados si el servicio de vMotion no está habilitado para ningún adaptador de VMkernel en la pila de TCP/IP predeterminada, o si ningún adaptador usa la pila de TCP/IP de vMotion.

8 Revise las modificaciones realizadas en la configuración y haga clic en **Guardar** para aplicar los cambios.

Quitar un adaptador de red de VMkernel en VMware Host Client

En VMware Host Client, puede quitar un adaptador de red de VMkernel en caso que ya no lo necesite.

Procedimiento

1 Haga clic en **Redes** desde el inventario de VMware Host Client y, a continuación, haga clic en **NIC de VMkernel**.

2 Haga clic con el botón derecho en el de adaptador de VMkernel que desea quitar y, a continuación, haga clic en **Quitar**.

3 Haga clic en **Confirmar** para quitar el adaptador de red.

Ver la configuración de la pila de TCP/IP en un host de VMware Host Client

Puede ver la configuración de DNS y de enrutamiento de una pila de TCP/IP en un host. También puede ver las tablas de enrutamiento IPv4 y IPv6, el algoritmo de control de congestión y la cantidad máxima de conexiones permitidas.

Procedimiento

1 Haga clic en **Redes** desde el inventario y, a continuación, haga clic en **Pilas de TCP/IP**.

2 Haga clic en una pila de la lista.

   Se muestran las opciones de configuración de la pila seleccionada.

Cambiar la configuración de una pila de TCP/IP en un host de VMware Host Client

Puede cambiar la configuración de DNS y de la puerta de enlace predeterminada de una pila de TCP/IP en un host. También puede cambiar el algoritmo de control de congestión, la cantidad máxima de conexiones y el nombre de las pilas de TCP/IP personalizadas.

Procedimiento

1 Haga clic en **Redes** desde el inventario de VMware Host Client y, a continuación, haga clic en **Pilas de TCP/IP**.

2 Haga clic con el botón derecho en una pila de la lista y seleccione **Editar configuración**.

   Se abre el cuadro de diálogo Editar configuración de TCP/IP: pila de aprovisionamiento.

3 Especifique el modo en que el host obtiene la configuración para esta pila de TCP/IP.

   - Seleccione el botón de opción **Usar servicios DHCP del siguiente adaptador** y, a continuación, seleccione un adaptador del que recibirá las opciones de configuración predeterminadas para la pila de TCP/IP.

- Seleccione **Configurar manualmente los valores de esta pila de TCP/IP** para modificar la configuración.

Opción	Descripción
Configuración básica	**Nombre del host** Edite el nombre de su host local. **Nombre de dominio** Edite el nombre del dominio. **Servidor DNS principal** Introduzca la dirección IP del servidor DNS de preferencia. **Servidor DNS secundario** Escriba una dirección IP del servidor DNS alternativa. **Buscar dominios** Especifique los sufijos de DNS para usarlos en la búsqueda de DNS al resolver un nombre de dominio sin calificar.
Enrutamiento	Edite la información de la puerta de enlace IPv4 e IPv6. **Nota** La eliminación de la puerta de enlace predeterminada puede generar una pérdida de conexión con el host.
Configuración avanzada	Edite el algoritmo de control de congestión y el número máximo de conexiones.

4 Haga clic en **Guardar**.

Configurar un firewall de ESXi en VMware Host Client

ESXi incluye un firewall que está habilitado de forma predeterminada. En el momento de realizar la instalación, el firewall de ESXi se configura para bloquear el tráfico entrante y saliente, excepto el tráfico de los servicios que están habilitados en el perfil de seguridad del host.

Al abrir puertos en el firewall, tenga en cuenta que el acceso no restringido a los servicios que se ejecutan en un host ESXi pueden exponer un host a ataques externos y acceso no autorizado. Para reducir el riesgo, configure el firewall de ESXi para que permita el acceso solo desde redes autorizadas.

Nota El firewall también permite pings del protocolo Control Message Protocol (ICMP) y la comunicación con los clientes DHCP y DNS (solo UDP).

Administrar la configuración del firewall ESXi mediante el VMware Host Client

Cuando inicia sesión en un host ESXi mediante el VMware Host Client, puede configurar conexiones de firewall entrantes y salientes para un servicio o un agente de administración.

Nota Si hay distintos servicios con reglas de puerto superpuestas, al habilitar un servicio, es posible que se habiliten otros servicios de forma implícita. Para evitar este problema, se pueden especificar qué direcciones IP tienen permiso para acceder a cada servicio en el host.

Procedimiento

1 Haga clic en **Redes** en el inventario de VMware Host Client.

2 Haga clic en **Reglas de firewall**.

   VMware Host Client muestra una lista de conexiones activas entrantes y salientes con los correspondientes puertos de firewall.

3 En algunos servicios, es posible administrar los detalles de servicio. Haga clic con el botón derecho en un servicio y seleccione una opción del menú emergente.

   - Utilice los botones Iniciar, Detener o Reiniciar para cambiar el estado de un servicio temporalmente.
   - Cambie la directiva de inicio para configurar el servicio de modo que este se inicie y se detenga con el host, los puertos de firewall o de forma manual.

Agregar direcciones IP permitidas a un host ESXi mediante VMware Host Client

De forma predeterminada, el firewall de cada servicio permite el acceso a todas las direcciones IP. Para restringir el tráfico, configure cada servicio para permitir el tráfico solo desde la subred de administración. También puede anular la selección de algunos servicios si el entorno no los usa.

Procedimiento

1 Haga clic en **Redes** desde el inventario de VMware Host Client y, a continuación, haga clic en **Reglas de firewall**.

2 Haga clic con el botón derecho en un servicio de la lista y haga clic en **Editar configuración**.

3 En la sección Direcciones IP permitidas, haga clic en **Solo permitir conexiones de las redes siguientes** e introduzca las direcciones IP de las redes que desee conectar al host.

   Separe las direcciones IP con comas. Puede utilizar los siguientes formatos de dirección:

   - 192.168.0.0/24
   - 192.168.1.2, 2001::1/64
   - fd3e:29a6:0a81:e478::/64

4 Haga clic en **Aceptar**.

Supervisar eventos y tareas de red en VMware Host Client

Puede ver detalles acerca de las tareas y los eventos asociados con los grupos de puertos, los conmutadores virtuales, los adaptadores de red físicos, los adaptadores de red de VMkernel y las pilas de TCP/IP en el host ESXi que está administrando.

Supervisar grupos de puertos en VMware Host Client

En VMware Host Client, puede supervisar el rendimiento de los grupos de puertos viendo los eventos y las tareas de los grupos de puertos en el host.

Procedimiento

1. Haga clic en **Redes** en el inventario de VMware Host Client.
2. Haga clic en **Grupos de puertos**.
3. Haga clic en un grupo de puertos de la lista.

   El grupo de puertos se expande en el inventario de VMware Host Client.
4. Haga clic en **Supervisar** bajo el nombre del grupo de puertos desde el inventario de VMware Host Client.
5. (opcional) Haga clic en **Eventos** para ver los eventos asociados con el grupo de puertos.

Supervisar conmutadores virtuales en VMware Host Client

En VMware Host Client, puede supervisar el rendimiento de los grupos de puertos viendo los eventos y las tareas de los conmutadores virtuales en el host.

Procedimiento

1. Haga clic en **Redes** en el inventario de VMware Host Client.
2. Haga clic en **Conmutadores virtuales**.
3. Haga clic en un conmutador virtual de la lista.

   El conmutador virtual se expande en el inventario de VMware Host Client.
4. Haga clic en **Supervisar** bajo el nombre del conmutador virtual desde el inventario de VMware Host Client.
5. (opcional) Haga clic en **Eventos** para ver los eventos asociados con el conmutador virtual.

Supervisar adaptadores de red físicos en VMware Host Client

En VMware Host Client, puede supervisar el rendimiento del adaptador de red físico viendo los eventos y las tareas de las NIC físicas en el host.

Procedimiento

1. Haga clic en **Redes** en el inventario de VMware Host Client.

2 Haga clic en **NIC físicas**.

3 Haga clic en un adaptador de red físico de la lista.

El adaptador de red físico se expande en el inventario de VMware Host Client.

4 Haga clic en **Supervisar** bajo el nombre del adaptador de red físico en el inventario de VMware Host Client.

5 (opcional) Haga clic en **Eventos** para ver los eventos asociados con el adaptador de red físico.

Supervisar adaptadores de red de VMkernel en VMware Host Client

En VMware Host Client, puede supervisar el rendimiento de los adaptadores de red de VMkernel viendo los eventos y las tareas de los adaptadores de red de VMkernel en el host.

Procedimiento

1 Haga clic en **Redes** en el inventario de VMware Host Client.

2 Haga clic en **NIC de VMkernel**.

3 Haga clic en un adaptador de red de VMkernel de la lista.

El adaptador de red de VMkernel se expande en el inventario de VMware Host Client.

4 Haga clic en **Supervisar** bajo el nombre del adaptador de red de VMkernel desde el inventario de VMware Host Client.

5 (opcional) Haga clic en **Eventos** para ver los eventos asociados con el adaptador de red de VMkernel.

Supervisar pilas de TCP/IP en VMware Host Client

En VMware Host Client, puede supervisar el rendimiento de las pilas de TCP/IP viendo los eventos y las tareas de estas pilas en el host.

Procedimiento

1 Haga clic en **Redes** en el inventario de VMware Host Client.

2 Haga clic en **Pilas de TCP/IP**.

3 Haga clic en una pila de TCP/IP de la lista.

La pila de TCP/IP se expande en el inventario de VMware Host Client.

4 Haga clic en **Supervisar** bajo el nombre de la pila de TCP/IP en el inventario de VMware Host Client.

5 (opcional) Haga clic en **Eventos** para ver los eventos asociados con la pila de TCP/IP.

6 (opcional) Haga clic en **Tareas** para ver las tareas asociadas con la pila de TCP/IP.